DOI: https://doi.org/10.56712/latam.v5i5.2691

El contexto actual e histórico de la ingeniería social

The current and historical context of social engineering

Jaime Junior Sedano Pinzón
jaime.sedano@gmail.com
https://orcid.org/0000-0002-0840-0733
Universidad Nacional Abierta y a Distancia
Vélez – Colombia

Artículo recibido: 09 de septiembre de 2024. Aceptado para publicación: 25 de septiembre de 2024.
Conflictos de Interés: Ninguno que declarar.

Resumen

En el presente artículo se presenta la ingeniería social tomando como base una indagación producto de revisión descriptiva, donde se ha identificado la manera como en el transcurrir del tiempo ha ido tomando gran relevancia los diferentes ataques haciendo uso de persuasión siendo muchos de los ataques e incidentes que se habrían podido evitar o mitigar si el usuario hubiera asumido una actitud más responsable con lo que se tiene y hace en tema de ciberseguridad. Los incidentes o amenazas tienen su origen y con el tiempo pueden ir quedando igual o mejorar, es por ello por lo que el problema es trabajado desde la pregunta ¿Qué se sabe de la ingeniería social desde su contexto actual e histórico?; por ser un tema de vital importancia, se empieza analizando el término “ingeniería social” desde el origen hasta la actualidad, seguidamente se pasa a revisión del funcionamiento, donde se tomaron técnicas más implementadas o significativas; algunas de ellas son: phishing, vishing, whaling, pharming, smishing, ataque en persona, entre otras; luego se exploran casos de la vida real y se presenta un análisis de una multinacional a nivel latinoamericano en cuanto a un tipo de ataque phishing durante el 2022 y se finaliza con medidas de acción y prevención para evitar ser víctima.

Palabras clave: persuasión, engaño, ataque, técnicas, malware

Abstract

This article presents social engineering on the basis of a descriptive review, where it has been identified how in the course of time has been taking great relevance the different attacks using persuasion being many of the attacks and incidents that could have been avoided or mitigated if the user had assumed a more responsible attitude with what you have and do in cybersecurity. Incidents or threats have their origin and over time they can remain the same or improve, that is why the problem is worked from the question "What is known about social engineering from its current and historical context? The first step is to analyze the term "social engineering" from its origin to the present day, followed by a review of its operation, where the most implemented or significant techniques were taken; some of them are: phishing, vishing, whaling, pharming, smishing, in-person attack, among others; then real life cases are explored and an analysis of a multinational company in Latin America is presented regarding a type of phishing attack during 2022 and ends with measures of action and prevention to avoid becoming a victim.

Keywords: persuasion, deception, attack, techniques, malware

Cómo citar: Sedano Pinzón, J. J. (2024). El contexto actual e histórico de la ingeniería social. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades 5 (5), 1357 – 1376. https://doi.org/10.56712/latam.v5i5.2691*

INTRODUCCIÓN

La presente investigación busca el reconocimiento de la ingeniería social desde el contexto actual e histórico, partiendo de los sistemas informáticos que no tienen un 100 % de seguridad plena; pero aunque se llegue a tener equipos tecnológicos que brinden seguridad, no implica que en muchas de las ocasiones sea el usuario quien llegue a convertirse en víctima o victimario, donde puede por un lado conseguir datos de otra persona sin darse cuenta está que los ha entregado, atendiendo a el artificio para que buenamente realicen acciones entre las que está, otorgamiento de permisos, la entrega de contraseñas, y múltiples actividades que normalmente no se harían, lo que lleva a que se use la llamada ingeniería social, conocida actualmente como un arte o manera de actuar de determinadas personas que busca la manipulación del ser humano utilizando infinidad de técnicas y métodos.

En el contexto actual la seguridad es demasiado a menudo solo una ilusión, que se vuelve peor aun cuando, "la ingenuidad, ignorancia o incredulidad entran en juego", la frase anterior redactada por Kevin Mitnick en su libro el Arte del Engaño, nos plantea la manera como algo que parece sólido puede convertirse en lo más frágil del mundo; es por ello que la presente investigación busca realizar una exploración de lo que se tiene actualmente y como ha sido su trascendencia en la historia de la ingeniería social, para dar respuesta a la pregunta ¿Qué se sabe de la ingeniería social desde su contexto actual e histórico? con el objetivo de realizar un análisis de cómo han evolucionado las diferentes formas de llevar a cabo un ataque para afectar la información.

El planteamiento del problema surge del ser humano que por naturaleza representa lo más frágil de la seguridad informática, tomando en cuenta que puede llegar a ser predecibles con la información que se tiene y maneja, muchos de los ataques cibernéticos acaecidos a lo largo de la historia se habrían podido evitar si se hubiera tenido una cultura preventiva antes de dar cualquier tipo de información. El saber reconocer las técnicas y cómo prevenirlas es de vital importancia al momento de gestionar políticas de seguridad informática.

METODOLOGÍA

En el presente ejercicio investigativo se parte de analizar una situación problemática donde intervienen tres elementos o factores: el ser humano, su manera de actuar y el medio por el cual se está actuando; estos se vuelven esenciales a la hora de la gestión de un producto o servicio, que para el caso actual es la información; seguidamente se exploran técnicas y casos de la vida real, donde la ingeniería social ha sido el eje principal del problema, llegando a proponer una recomendaciones en pro de sensibilizar al usuario para que no se vuelva una víctima más.

DESARROLLO

La persuasión

Cuando se piensa en seguridad sea cual sea su escenario, un elemento clave a la hora de su implementación es el ser humano, donde puede llegar a representar un riesgo al momento de tener que actuar, viéndose ciertamente influenciado por lo que se conoce como la persuasión, que es definida por (Castillero Mimenza, 2016) como "el proceso mediante el cual se emplean mensajes a los cuales se dota de argumentos que los apoyen, con el propósito de cambiar la actitud de una persona, provocando que haga, crea u opine cosas que originalmente no haría, crearía u opinaría"; para poder llevar a cabo la persuasión se hace uso de seis principios definidos por Robert Cialdini como: 1) Reciprocidad, 2) Compromiso y coherencia, 3) aprobación social, 4) Empatía, 5) Autoridad, 6) Escasez.

Figura 1

Los 6 principios de la persuasión de Cialdini

Fuente: Los 6 principios de la persuasión de Cialdini aplicadas al inbound marketing https://www.inboundcycle.com/blog-de-inbound-marketing/los-6-principios-de-la-persuasion-de-cialdini-aplicadas-al-inbound-marketing

Una persona con habilidades para persuadir puede hacer que se ponga en riesgo toda una organización gracias a diferentes técnicas de ingeniería social que hacen uso de la persuasión, por lo que es importante conocer su funcionamiento.

¿Qué se entiende por Ingeniería Social?

El término ingeniería social tiene sus orígenes en los pensadores liberales con conceptos filantrópicos hacia mediados del siglo XIX, donde se da inicio a través de un ensayo del empresario holandés J.C. Van Marken, siendo difundido por Émile Cheysson; ya en la política la expresión asume varios sentidos, uno en relación con esfuerzos para la influencia de actitudes, relación o acciones sociales sobre población de una nación o región y otro basado en implementación en programas de transformaciones sociales.

En un comienzo las empresas hacían uso del término ingeniería social para tratar a la persona que tenía la función de mediador en la resolución de conflictos, el cual ejercía intermediación racional entre el capital y el trabajo; pero es en 1945 que la expresión es reintroducida por parte de Karl Popper, convirtiéndose en un método o técnica para el logro de una gran multiplicidad de resultados, dejándose de lado como instrumento de solución de pugnas sociales para transformarse en manipulación de personas, estos delincuentes o hackers eran inicialmente llamados phreakers (Phone + hack + freak) enfocados en saber cómo es el funcionamiento de la telefonía y el manejo de sistemas de comunicación abarcando desde las compañías hasta la tecnología. Desde la ICDE.ORG.CO se plantea que cuando se obtiene información delicada de otro usuario sin que este sepa, se está incurriendo en ingeniería Social (IS) como una doctrina.

Figura 2

John Draper y el origen de los Phreaks

Nota: Jorge M. (2016) John Draper, unos de los primeros Phreaks.

Funcionamiento de la ingeniería Social

Cuando se habla de ciberataques se tienen en muchas ocasiones ideas erróneas, pensando que solo se necesitan herramientas y tecnología sea avanzada o no de hackeo para la irrupción en computadores, equipos móviles o cuentas de usuarios, lo que lleva a que se cometan errores y a través de una de las trampas preferidas como lo es la lectura en frío se engañe al usuario y termine otorgando información reservada.

Ahora, el ser humano es conocido por naturaleza como el eslabón más débil de la cadena en seguridad informática, porque si bien el tener un sistema ultra seguro, no implica ser una garantía de seguridad al 100 %; ya que tomar una decisión en un momento dado es en base a eventos o acciones que se presenten, siendo un ejemplo claro los correos sobre tormentas en Europa 2007 donde se usó la Ingenuidad, la curiosidad y la morbosidad humana (Barrera Ibañez, 2013), y es la ingeniería social a través de la persuasión y la influencia que un usuario puede llegar a realizar una determinada acción de modo erróneo.

El desarrollo de un ataque de ingeniería social se lleva a cabo en muchos de los casos, a través de mensajes verídicos y fuentes fidedignas que hagan despertar la confiabilidad en el usuario, lo que hace que la recolección de información y/o la expansión de malware sea todo un éxito, gracias a una estructura funcional básica esquematizada en una serie de pasos a través de ciclos, los cuales se pueden visualizar en la figura 3.

Figura 3

Pasos ciclo de ataque de ingeniería social

Nota: El ciclo básico de un ataque de ingeniería social hace uso de cada paso, de modo tal que se logre el objetivo, si no se consigue en el primer intento se repite nuevamente, la descripción de cada uno de ellos se describe en la tabla 1, partiendo de la investigación hasta llegar al lanzamiento del ataque.

Tabla 1

Pasos utilizados dentro de la ingeniería social

Investigación	Se procede a realizar la recolección de información, ya sean estos informes, material, datos de la víctima y todo aquello que busque el lograr construir un anzuelo exitoso que lleve a determinar la mejor forma de acercarse al objetivo construyendo relaciones.
Anzuelo	Después de ejecutar la investigación, se procede a iniciar la farsa, construyendo un grado de intimidad, con la víctima y se toma control de la interacción.
Desarrollar rapport y credibilidad	Teniendo como base los datos obtenidos anteriormente, se cambian las identidades y se le exige a la víctima, lo que puede ser un apoyo o hacer uso de la autoridad.
Aprovechamiento de confianza	Se consulta o logra que te pregunten con tal de extraer información y mantener las cosas con el suficiente tiempo, manteniendo la farsa hacia la víctima y se extrae información.
Utilizar información	Se cierra la interacción buscando no despertar sospecha, si se consigue solo una parte de la información, se procede a repetir el ciclo con tal de lograr el objetivo y se provee al usuario de las razones para guardar silencio.
Lanzar Ataque a Sistema	Paso donde por medio de un ransomware, un cryptolocker o un troyano de diversa índole, se busca ya sea dañar y secuestrar datos sensibles en el sistema.

Fuente: MITNIK Kevin, El arte del engaño, 2001.

Técnicas de Ingeniería Social

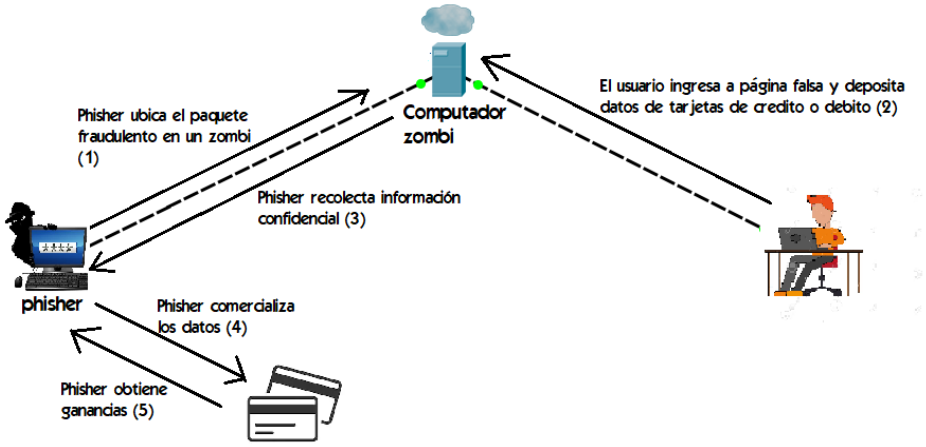
Al momento de querer acceder a información o realizar algún tipo de ataque, se puede hacer uso de múltiples técnicas donde la Ingeniería Social comienza a ser aplicada por medio de códigos maliciosos y otro tipo de atacantes. Cuanto más real parezca el mensaje, más confiable sea la fuente y más crédulo sea el usuario, mayores posibilidades tendrá el atacante de concretar con éxito sus propósitos (Borghello, 2009), siendo muy conocidas las siguientes:

Phishing

Técnica en la que los cibercriminales buscan engañarte para llevar a cabo una acción. Su inicio suele ser en su mayoría con el envío de correo electrónico, pretendiendo ser alguien o algo que se conoce o es confiable, como tiendas en línea, banco o amistad, a través de estos mensajes te motivan a realizar algún evento como ingresar a un enlace, abrir archivo adjunto o responder mensaje, todo a modo que parezca convincente, enviándolos a miles de usuarios a nivel mundial.

Figura 4

Pasos ataque de phishing



Fuente: Pasos de ataque de phishing - Google.com.co.

Whaling phishing

También conocido como Whale phishing es un tipo específico de ataque que se dirige a empleados que tienen un alto perfil, como los CEO, buscando el robo de información, si la cuenta de correo electrónico de la administración llega a estar comprometida, puede ser explotada para ataques contra empleados o incluso fuera de la organización.

Figura 5

¿Qué es el Whale phishing?

Nota: ¿Qué es el whale phishing? - https://www.ibm.com/mx-es/topics/whale-phishing

Spear-Phishing

Estafa de correo electrónico dirigida a personas, organizaciones o empresas específicas buscando robar información a su vez se puede tratar de instalar Malware en el equipo de la víctima. El manejo inadecuado de los datos que se reciben por email puede poner en riesgo a toda la organización (Karpersky Lab, s.f.).

Figura 6

Pasos ataque de spear-phishing

Fuente: Spear Phishing Explained. https://us.norton.com/blog/online-scams/spear-phishing

Smishing

Tipo de phishing a través del cual tiene como objetivo conseguir información privada por medio de mensaje de texto SMS o número de teléfono. Los atacantes buscan datos desde contraseñas hasta

información de tarjetas de crédito y débito, muchos de los métodos usados es el miedo donde son recibidos enlaces con carácter urgente (Norton, 2018).

Figura 7

Ataque smishing

Fuente: 'Smishing': cómo evitar este ciberataque a través de SMS, https://www.redseguridad.com/actualidad/cibercrimen/smishing-como-evitar-este-ciberataque-a-traves-de-sms_20220408.html

Vishing

Unión entre voice + phishing o también conocido como suplantación de voz o telefonía, basado en el aprovechamiento de VOIP donde se brinda un número telefónico falso aparentando ser el verdadero y conseguir datos sensibles ya sea contraseñas, claves de tarjetas tanto de crédito como débito y nombres de usuarios, con el vishing se capitaliza la confianza de una persona en el servicio telefónico, ya que la víctima generalmente no asume que el estafador tiene gran capacidad en el uso de técnicas como spoofing y sistemas automatizados avanzados (Yeboah & Mateko, 2014, p. 300).

Figura 8

El Vishing

Fuente: ¿Sabes qué es el 'vishing'?, https://computerhoy.com/ciberseguridad/sabes-vishing-tipo-estafa-cada-vez-popular-puede-acabar-intimidad-1320892

Help Desk

Ataque en el cual a través de brindar ayuda se busca el ingreso y obtención de información clasificada, dentro de las características encontramos el poder ingresar fácilmente, Se desea siempre brindar ayuda, el nuevo empleado en la empresa busca recibir apoyo, por medio de enlace remoto, Representación de recursos humanos, Personal de IT de otra localidad o empresa. Ejemplo: Atacante: Hola, perdón soy un empleado nuevo y no recuerdo la contraseña asignada.

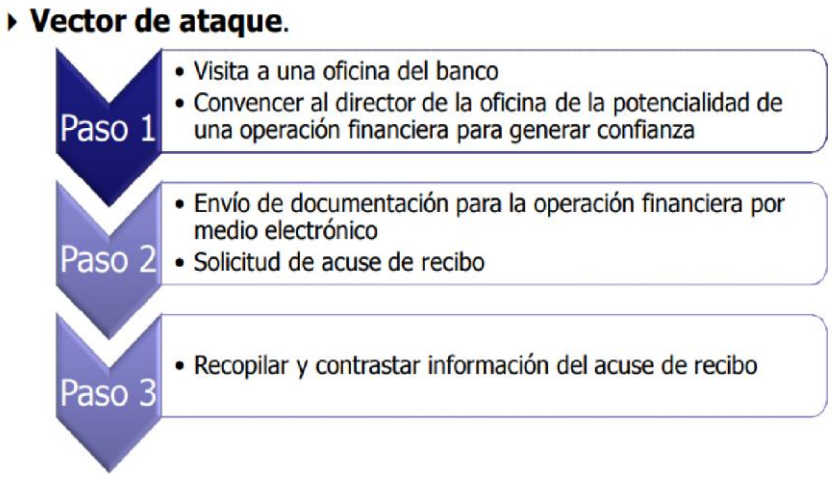
Víctima: Por supuesto, te voy a brindar mi clave hasta que te den nuevamente la tuya.

Ataque en persona

Tipo de ataque en el cual una persona se hace pasar como empleado y solicita información para el acceso a sistema, un ejemplo de ataque en persona puede verse en la siguiente figura:

Figura 9

Pasos ataque en persona



Fuente: Caso 1 Asaltando un Banco, https://docplayer.es/15753809-Owand-11-granada-ingenieria-social.html

Quid Pro Quo

Ataque en el cual se ofrece beneficio a las víctimas, pero tienen que otorgar información a cambio, de nombres de usuarios, contraseñas o productos (Alzas Hernandez, 2023), un procedimiento que se ha implementado en cantidad es el relacionado con el soporte técnico donde se llama para ofrecer el servicio y solventar el problema, pero pide credenciales de login (López Grande & Guadrón, 2015).

Dumpster Diving

Ataque en el cual se ofrece a la víctima beneficios a cambio de información delicada de organización o el mismo usuario. donde se investiga a un empleado y se plantea incentivos, pero debe dar datos críticos.

Las cartas nigerianas

También conocido como `timo 419´, proviene del número del artículo del código penal que se vulnera en Nigeria (Arcos Sebastián, 2011), son mensajes falsos invitando a conseguir una gran cantidad de

dinero a cambio de un desembolso inicial, un caso muy dado es el de la herencia millonaria que ha tenido la gentileza de compartir con nosotros, también se puede presentar el premio de lotería con el que hemos sido agraciados sin haber jugado.

Shoulder surfing

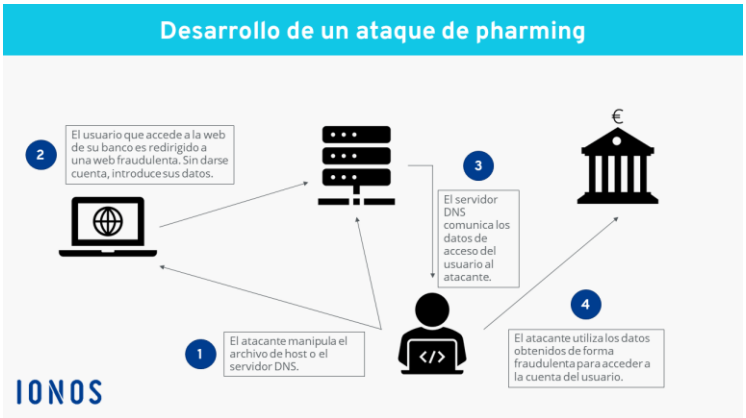
Técnica de mirar por encima del hombro, donde el usuario es espiado para obtener nombre de usuario y contraseña a través de la observación directa de lo tecleado en el ordenador o dispositivo, el éxito reside en la sencillez y paciencia del atacante y mediante la tecnología de hoy en día, el atacante puede hacer uso de diferentes dispositivos con el fin de conseguir información directa (Gil Lluís, 2022, p. 38).

Pharming

Consiste en que, estando el ordenador infectado por un código malicioso o software se posibilita la realización de cambios a DNS, al momento de intentar acceder a una página web se introduce la URL y confiando que es el sitio web deseado, se procede a realizar compras o cualquier otra transacción electrónica llevando a que el atacante obtenga claves de seguridad y la puerta abierta al fraude (Callegari, 2007, p. 176).

Figura 10

Desarrollo de un ataque de pharming



Fuente:¿Qué es el pharming?, https://www.ionos.es/digitalguide/correo-electronico/seguridad-correo-electronico/que-es-el-pharming/

Spam

Emails no deseados, los cuales pueden llevar publicidad, virus u otro fin, los remitentes suelen ser desconocidos o no incluidos en libreta de direcciones y a través de la toma de una decisión se pretende engañar al usuario para acceder a un enlace o descargar un archivo malicioso.

Figura 11

Spam

Fuente: SPAM desde Rusia y China: Solución a los ataques de formulario, https://www.mundiserver.com/spam-solucion-los-ataques-formulario/

Softwares implementados en Ingeniería Social

A nivel mundial se han implementado múltiples softwares en el desarrollo de ataques de ingeniería social, dos de estos han sido utilizados en un momento dado implicando pérdidas significativas, estos son:

Malware Android.FakeTrojan.A

Malware que suele estar en software el cual se muestra al usuario haciendo creer que es un software confiable para la generación de acceso único tipo token de banca en línea. La aplicación se adapta a múltiples entidades bancarias con logos y colores reales.

Figura 12

Ejemplo Malware Android Fake Trojan

CryptoLocker

A través del cryptolocker se busca que el mismo usuario lo ejecute donde el usuario accede a un correo que recibe y aparenta ser de una organización confiable, donde se incluye un archivo comprimido tipo

ZIP con una contraseña, este ransomware tiene un patrón de negocio fundamentado en la extorsión al usuario.

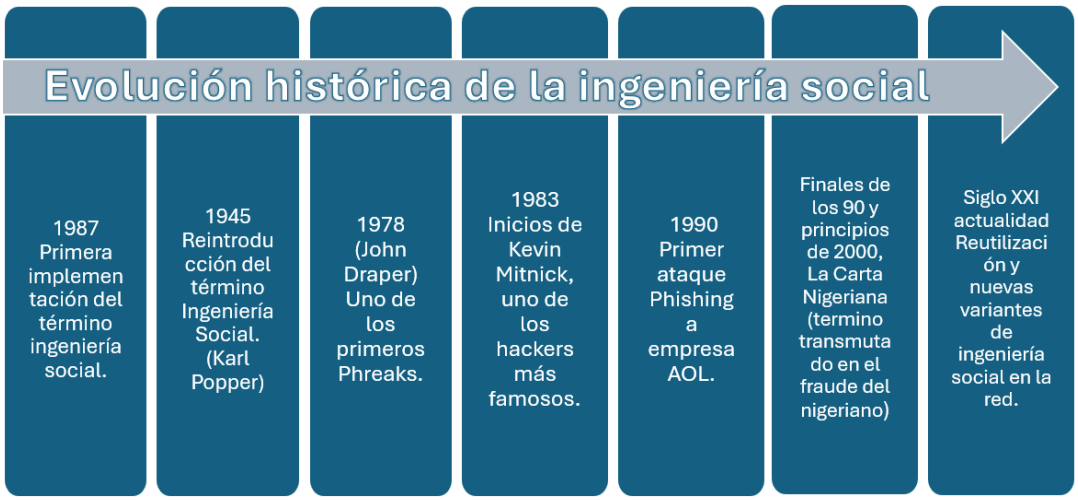
El proceso de instalación es llevado a cabo en la carpeta del perfil AppData o LocalAppData, pasando luego a ejecutarse al reiniciar el equipo por medio de un autorun y se asegura lanzando dos procesos un principal y un secundario ante posible cierre.

Evolución histórica de la Ingeniería Social

A medida que ha ido avanzando la historia, la ingeniería social desde el término hasta las acciones han ido tomando diferentes connotaciones influyendo en una u otra forma los avances tecnológicos, teniendo en cuenta el origen del término y los múltiples ataques que se han visto, se realiza un breve análisis de cómo ha evolucionado.

Figura 13

Evolución histórica de la ingeniería social



Nota: Recorrido de la ingeniería social desde el surgimiento en 1987 hasta la actualidad (Autor propio).

Casos de ingeniería social en el mundo

Agnus Young

Agnus un joven de tan solo 14 años, con un teclado que mantenía cubierto por típex blanco y entintado con color fluorescente que rotulador, escuchando música de la Polla Récord o Kortatu, se dedicaba a recorrer las líneas telefónicas del mundo desde su ordenador "Amiga 500" con un altavoz roto pegado al micrófono de carbón de un teléfono. Era una persona que sabía mucho de Phreaking en España, escribía documentos de cómo actuaba donde los demás hackers lo implementan para llamar gratis a cualquier lugar.

D-Orb

Una señora que se ubica en una tienda de modas se acerca a la caja con múltiples prendas acompañada de su hija la cual tenía una edad de 14 años, la cajera realiza la suma total de la adquisición y procede a entregar la tirilla y luego la cliente saca su tarjeta MASTERCARD para el pago. La cajera coge la tarjeta y la pasa por la máquina lectora e imprime los datos, seguidamente procede a llamar a la central de autorizaciones de la empresa a la cual pertenecía la tarjeta y consulta, al final

le entrega la tirilla a la cliente. D-Orb ubicado cerca de un aparador detalla toda la operación llevada a cabo, cuando la mujer sale de la tienda este se dirige hacia un establecimiento en frente y llama al número que lee por fuera de las bolsas que lleva la cliente.

¿Buenos días señora me contestan de "Virginia Moda"? con voz seca en el auricular.

Si, ¿En qué le puedo servir?

Mi nombre es Carlos González y le estoy llamando del centro de autorizaciones de MASTERCARD ¿Puede usted confirmar su número de tienda?

Por supuesto Don Carlos es el KU987.

Perfecto está todo bien, como verá usted, se han presentado problemas con la autorización que solicitaste hace un par de minutos. ¿Podría repetir nuevamente los datos que le pediré del comprobante?

Dame un momento mientras busco el comprobante Don Carlos.

¿Cuál es el número de la tarjeta?

Si, el número es 3456 8765 2345 1234

¿Nombre del titular tal cual como está escrito?

Luisa Simpson.

¿La fecha de caducidad es?

08/90

Ok muchas gracias, procederé a procesar la operación inmediatamente, gracias por su ayuda buenos días.

La interlocutora no presentó ninguna duda de lo que estaba brindando al hacker, sin tener en cuenta que los datos podrían ser utilizados en cualquier lugar del mundo.

Omega

Omega era conocido el hacker que se dedicaba a corroborar de modo periódico los cajetines de telefonía para identificar la incorporación de nuevos números (pares conectados), estudiando diversos edificios en el centro de la ciudad por muchos meses. La verificación la realiza por medio de un software "wardialing" (Encargado de realizar llamadas automáticas a números de teléfono y guardaba los resultados en bases de datos).

Hacker Ciego al FBI año 2005

En EE.UU., la central de emergencias recibe una llamada por la línea 911 donde escuchan lo siguiente: Pon mucha atención, en estos momentos tengo a dos rehenes ¿de acuerdo' ¿Entiendes que les sucede a las personas que suelen ser rehenes? una pista: no terminan como en el cine. Te diré, uno se llama Danielle, el otro es su padre. Esto lo hago por una sencilla razón, y es porque su papá violó a mi hermana dejándola inconsciente.

El atacante se identifica como John Defanne. Desde la central se realiza la verificación del número y se trata de la casa de los papás de Danielle, ubicada en un suburbio de Colorado Spring. Desde el otro lado de la línea Defanne continúa hablando. Estoy armado, tengo un revólver. Les dispararé sin dudarlo.

La fuerza pública sale disparada rumbo a la casa y llegan en contados minutos. Los oficiales se preparan para un gran enfrentamiento armado con el sospechoso homicida. Pero cuando entran se llevan una gran sorpresa. No hay ningún homicida armado en su interior, ni rehenes, ni una sola gota de sangre. Danielle y su papá estaban viendo la televisión tranquilamente en la sala. Ellos nunca habían oído hablar de John Defanne.

Grupo Carbanak

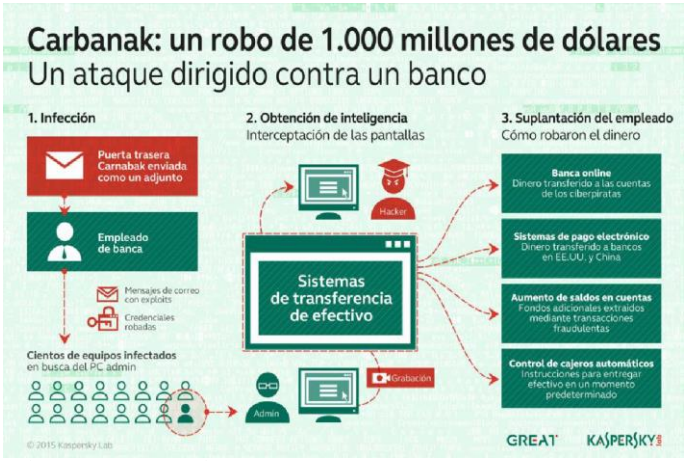
Carbanak, conocida como puerta trasera diseñada para tareas de espionaje, extracción de datos y control remoto de equipos, ciberdelincuencia combinada, donde se realizó robo de dinero a instituciones financieras, con técnicas de infiltración por medio de ataques dirigidos. La operación fue descubierta en 2015, debido a que una entidad financiera contrató a Kaspersky Lab para conducir una investigación forense de los sistemas bancarios debido a que los cajeros automáticos entregaban dinero de forma indiscriminada. Resultado de ello se detecta una infección.

Los atacantes usaron métodos de los APTs para infectar, como el envío de mensajes de e-mail spear-phishing a funcionarios bancarios. Una vez se lograba la captura del ordenador, los delincuentes cibernéticos llevaban a cabo actividades de inspección para identificar sistemas de procesamiento, cajeros automáticos, contabilidad o sencillamente replicaban las actividades de los empleados. Carbanak recurrió a tres métodos los cuales son: transferencias a cuentas de los delincuentes, entrega de dinero en cajero automático, cuentas falsas y multas para recolectar dinero. Más de 100 entidades financieras se vieron afectadas, cuyas pérdidas ascienden a más de mil millones de dólares.

En un gráfico presentado por la multinacional Kaspersky Lab, se puede evidenciar cómo se desarrollaron los ataques que dejaron pérdidas de 1000 millones de dólares.

Figura 14

Ataque Carbanak



Nota: Ataque Carbanak (Kaspersky Lab)

Ingeniería social inversa en caso Ubiquiti Networks

Ubiquiti Networks es una empresa de EEUU la cual brinda servicios de redes para empresas con un alto rendimiento. Para el año 2015 la compañía sufrió un ataque que le implicó perder 39.1 millones de dólares. Los cibercriminales se hicieron pasar por funcionarios de la empresa y realizaron solicitudes de transferencia de grandes cantidades de dinero al área financiera hacia una cuenta bancaria particular de propiedad de los ciber-delincuentes.

Toda la brecha de seguridad en este caso estuvo en los propios empleados, no se necesitó el ingreso al sistema informático, tampoco se perdieron datos de la compañía. La carencia de la formación y desconocimiento de procedimientos necesarios permitió que se llevarán a cabo este tipo de estafas.

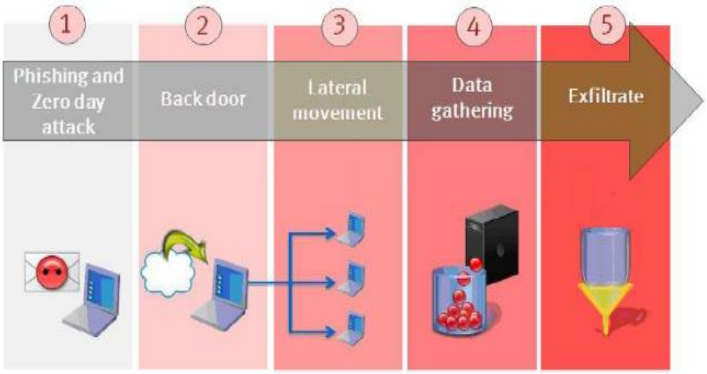
Ataque a RSA en 2011

El ingreso al sistema RSA se llevó a cabo por medio del uso de CVE-2011-0609, una deficiencia de seguridad en Flash que estaba siendo explotada de forma activa a través de la incrustación de ficheros en Excel. para lograr infiltrarse enviaron e-mails a empleados con un nivel bajo en la escala RSA y uno de ellos lo rescato de la junk folder buscando abrir el fichero Excel adjunto y su contenido.

La apertura de ficheros ofimáticos que vienen adjuntos en emails son una constante de muchos usuarios que tienen las defensas bajas ante archivos PDF, Excel y ODF. Cuando es explotada la vulnerabilidad se instala una versión modificada de Poisson Ivy, una de las RAT más famosas, la cual permite: encender la cámara, realizar conexiones desde la víctima hasta el atacante.

Figura 15

Ataque a RSA (Chema alonso)



Fuente: Ataque a RSA (Chema Alonso).

Hurto de más de 1 millón de dólares por parte de Dyre Wolf

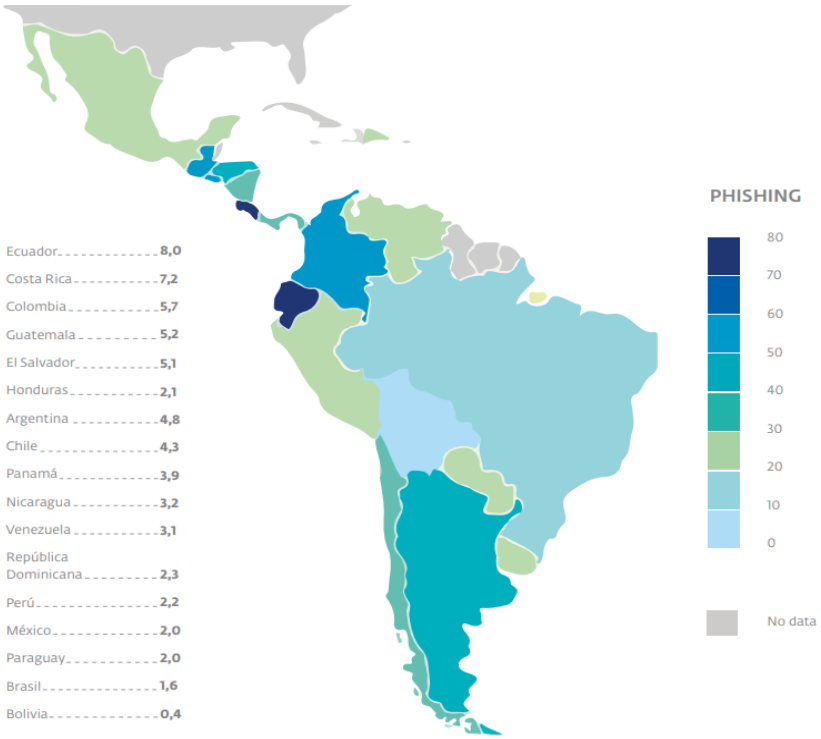
El ataque se desarrolló iniciando con un phishing de e-mail que llega a la empresa con un archivo adjunto que hace creer que tiene importancia económica, pero realmente es un Upatre downloader, una vez se abre, descarga y ejecuta el troyano Dyre en el equipo de la víctima. La mayoría de los programas antivirus no lo detectaron. A través del Malware se vigila las actividades de la víctima y pasa a modo espera, cuando la víctima intenta iniciar sesión, Dyre muestra una nueva pantalla con un mensaje indicando que el sitio está experimentando fallas y se debe llamar al número proporcionado para adelantar la transacción (The hacker News, 2015).

Análisis ataques phishing durante el 2022

El devenir de la tecnología y su rápido crecimiento ha hecho que a la par se presenten múltiples amenazas a mundial las cuales han evolucionado, dejando de lado el solo software que se dedicaba a dañar sistemas operativos para pasar al uso de técnicas de ingeniería social y lograr acceder a información dañando sistemas y es la multinacional ESET Security quien presenta un reporte de incidencia asociado a ataques Phishing en Latinoamérica del año 2022, los cuales se presentan en la siguiente tabla:

Figura 16

Incidentes en Latinoamérica de phishing 2022



Fuente: (ESET) Países de América Latina con mayor cantidad de detecciones de phishing en 2022, https://web-assets.esetstatic.com/wls/es/articulos/reportes/eset-security-report-latam2023.pdf

Las cifras presentadas por la multinacional ESET dejan ver como a nivel latinoamericano se han presentado gran cantidad de ataques de ingeniería social tipo phishing durante el año 2022, presentando un mayor porcentaje en el Ecuador.

Medidas de acción y prevención de Ingeniería Social

Un sentido de urgencia impreso por alguien: El tener que tomar decisiones bajo presión en un momento dado debe hacer sospechar de un posible ataque.

Si se solicita información que no deberían tener o que ya tendrían que conocer por defecto, tome las medidas preventivas a las que haya lugar y no otorgue datos.

Algo excesivamente bueno verdadero. Puede darse con empresas que ofrecen intereses extraordinarios o incluso cuando te indican que ganaste la lotería, pero no la juegas, no todo lo que parece ser bueno es real, evite las trampas.

Para tener una tranquilidad y nivel de seguridad aceptable, es recomendado NUNCA responder a requerimientos de información personal por ningún medio sea teléfono, mensaje corto (MSN) o correo electrónico.

Ninguna entidad sea bancaria o de otra índole le solicita información como tarjetas de crédito, contraseñas vía correo electrónico o llamada, ellos tienen ya los datos. Si se le olvida o pierde usted puede realizar la solicitud directamente con ellos.

Un procedimiento seguro para el acceso a sitios web, es teclear el dominio de la página web en la barra de direcciones del browser, nunca utilice enlaces que sean de cualquier procedencia, las entidades tienen certificado y cifrado seguro.

Evite abrir correos electrónicos no solicitados o que sean de una procedencia dudosa o poco conocida. Los códigos malignos que alteran la configuración del sistema para llevar a cabo ataques de pharming, por lo general suelen venir a través de otro software malicioso, gusanos o troyanos que después de adelantar el ataque desaparecen dejando un enorme agujero de seguridad en el PC con conexión a internet.

Utilice protecciones integrales que le permitan la prevención de ataque maliciosos, dentro de estas soluciones se debe hacer uso de antivirus (Con disponibilidad de acceso a internet para mantener la base de datos actualizada), un firewall con políticas debidamente configuradas para acceso y salida de datos, una herramienta para la detección de correo no deseado (spam) y contra programas espía, además configurar niveles de protección de redes WIFI, valoración de vulnerabilidades en sistema y control de tipo de sitios web.

Tome medidas preventivas en navegación cotidiana para evitar la pérdida de confianza en el uso de herramientas de la banca en línea o comercio electrónico, ya que estos han generado grandes beneficios económicos a nivel mundial.

DISCUSIÓN

Teniendo como base la revisión histórica desde el origen de la ingeniería social y los diferentes tipos de ataques que puede sufrir una persona, hace que se llegue a la conclusión donde el sufrir un ataque como el phishing u otro puede ser llevado a cabo de diferentes formas y el utilizar software para ataques cibernéticos puede hacerse a través de múltiples técnicas de expansión, por lo que las medidas de prevención en ingeniería social tienen que abarcar diferentes escenarios donde se puede ver afectada la información y es lo que le pudo haber faltado a aquellas empresas que a lo largo del tiempo se han visto involucradas en incidentes cibernéticos a causa de diferentes formas de atacar al eslabón más débil de la cadena en seguridad informática como lo es el usuario final que no depende de un país en específico y es lo que dejó ver el reporte presentado por la multinacional ESET en solo Latinoamérica en este caso; pero con la rápida expansión del internet su alcance es mundial.

CONCLUSIÓN

Si bien el funcionamiento base de un ataque de ingeniería social arranca con un proceso de investigación hasta el lanzamiento de ataque, puede que no se tenga que esperar a desarrollar todo un proceso y simplemente se proceda con la aplicación directa de un tipo de ataque, por lo que saber reconocer los diferentes ataques y el asumir una posición de aprendizaje permanente es indispensable para cualquier usuario, desde cómo evitar la aplicación de la persuasión en contra y conocer las últimas técnicas sin dejar de lado lo que se tiene en auge en estos momentos que es la Inteligencia Artificial la cual entrará a convertirse en un nuevo escenario para el ataque y la defensa.

REFERENCIAS

Alzas Hernandez, J. (2023). Estudio de fraudes basados en la técnica de Ingeniería Social [masterThesis, Universitat Oberta de Catalunya]. https://openaccess.uoc.edu/handle/10609/148147

Arcos Sebastián, S. (2011). Ingeniería social: Psicología aplicada a la seguridad informática [Proyecto/Trabajo final de carrera, Universitat Politécnica de Catalunya]. https://upcommons.upc.edu/handle/2099.1/12289

Barrera Ibañez, S. (2013). La ingeniería Social y Cibercrimen. Seguridad y Ciudadanía: Revista del Ministerio del Interior, 10, 11-27. https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/seguridad-y-ciudadania/Seguridad_y_Ciudadania_N_10_web_12613037X.pdf

Biscione, C. (NN). Ingeniería Social para no Creyentes [Presentación electronica]. https://acis.org.co/portal/sites/all/themes/argo/assets/img/Pagina/IngenieraSocial_CarlosBiscione.pdf

Borghello, C. (2009). El arma infalible: La Ingeniería Social [Manuscrito de prensa]. http://www.eset-la.com/pdf/prensa/informe/arma_infalible_ingenieria_social.pdf

Callegari, O. (2007). Delitos informáticos: Pharming. Negocios de Seguridad, 31, 176-176. http://www.rnds.com.ar/revistas/031/RNDS_031.pdf

Castillero Mimenza, O. (2016). Persuasión: Definición y elementos del arte de convencer [Pagina Web Dinamica]. Psicología y Mente. https://psicologiaymente.com/social/persuasion-definicion-elementos-convencer

ESET (2023) Security Report Latinoamérica https://web-assets.esetstatic.com/wls/es/articulos/reportes/eset-security-report-latam2023.pdf

Gil Lluís, L. A. (2022). Estudio de los ataques y su defensa en la Ingeniería Social [Tesis fin de Master, Universidad Nacional de Educación a Distancia (España)]. https://hdl.handle.net/20.500.14468/21398

Jorge M. (2016) John Draper, unos de los primero Phreaks. https://es.gizmodo.com/pioneros-de-la-ingenieria-social-el-hacker-ciego-que-p-1789268307

Karpersky Lab. (SF) ¡Que es el Spear phishing?. https://latam.kaspersky.com/resource-center/definitions/spear-phishing

López Grande, C. E., & Guadrón, R. S. (2015). Ingeniería Social: El Ataque Silencioso. Revista Tecnologica, 8, 38-45. https://www.itca.edu.sv/wp-content/themes/elaniin-itca/docs/RevistaTec_N8_Digital.pdf

Norton (2018) ¿Qué es el smishing?, Norton Colombia, https://co.norton.com/internetsecurity-emerging-threats-what-is-smishing.html

Rincón Nuñez, P. M. (2023). Ataques basados en ingeniería social en Colombia, buenas prácticas y recomendaciones para evitar el riesgo. InterSedes, Revista electrónica de las sedes regionales de la Universidad de Costa Rica, 24(49), 120-150. https://www.scielo.sa.cr/pdf/is/v24n49/2215-2458-is-24-49-120.pdf

The hacker News (2015), Dyre Wolf roba más de 1 millón de dólares por transacción, Disponible en: https://www.seguridad.unam.mx/historico/noticia/index.html-noti=2216

Yeboah E. & Mateko P. (2014) Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices, Journal of Emerging Trends in Computing and Information Sciences. https://e-tarjome.com/storage/btn_uploaded/2020-09-12/1599891065_11216-etarjome%20English.pdf