LA INGENIERÍA SOCIAL, EL ANTES Y EL AHORA DE UN PROBLEMA GLOBAL

JAIME JUNIOR SEDANO PINZÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
VÉLEZ, COLOMBIA
2019

LA INGENIERÍA SOCIAL, EL ANTES Y EL AHORA DE UN PROBLEMA GLOBAL

JAIME JUNIOR SEDANO PINZÓN

Trabajo de monografía presentada(o) como requisito parcial para optar al título de:
Especialista en Seguridad Informática

Director (a):

Ingeniero de Sistemas EDGAR MAURICIO LÓPEZ ROJAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
VÉLEZ, COLOMBIA
2019

Nota de Aceptación

_____
_____
_____
_____
_____
_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Vélez 26 de julio de 2019

Dedicatoria

El presente trabajo es dedicado a Dios por llenarme de Fe, paciencia y sabiduría, a mi madre Gloria Esperanza Pinzón, todos; que de una u otra forma me han estado motivando y apoyando de modo incondicional para alcanzar este gran logro en mi vida.

AGRADECIMIENTOS

Sin lugar a duda agradezco de todo corazón la colaboración y exalto su inmensa labor, a todas aquellas personas que de una u otra forma aportaron el granito de arena para el desarrollo del presente trabajo, entre ellas a mis compañeros tutores que me tuvieron paciencia en algunos momentos cuando se requirió.

Al director RUBIEL SUAREZ GONZALEZ por su motivación para que desarrollará la especialización en Seguridad Informática y por supuesto, a la UNAD CEAD VÉLEZ. A todas las personas entre amigos, familiares y demás allegados.

Muchas gracias a todos…

RESUMEN

Durante la indagación realizada se ha identificado la manera como la ingeniería social con el transcurrir del tiempo ha ido tomando gran relevancia en el mundo de la ciberseguridad, muchos ataques e incidentes causados podrían haberse evitado, si el ser humano hubiera asumido una actitud más responsable con lo que debe saber, primordialmente basado en lo intelectual y seguidamente su instinto. Los problemas o amenazas tienen su origen y con el tiempo pueden ir quedando igual o mejorar; es por esto que surge la pregunta ¿Cuál ha sido la evolución que ha tenido la ingeniería social entre 1950 hasta 2017 y que consecuencias se han visto?

Después de tener planteada la problemática, la revisión se orientó hacia la identificación de técnicas de ingeniería social, entre las que se encuentran: phishing, scam, whaling, pharming, smishing, ataque en persona, entre otras; luego se analizó como estas han avanzado en el tiempo para llegar a las medidas preventivas, en pro de generar conciencia frente al manejo adecuado de la información que se genera diariamente. Finalmente, después de un amplio recorrido bibliográfico, se concluye con un conjunto de sugerencias para evitar ser víctima de ingeniería social.

Palabras Clave:
ENGAÑO, MANIPULACIÓN, DELINCUENTES, MALWARE, RAMSONWARE

ABSTRACT

During the inquiry conducted has been identified how social engineering with the passage of time has been taking great relevance in the world of cyber security, many attacks and incidents caused could have been avoided if the human being had assumed a more responsible attitude with what you should know, primarily based on the intellectual and then your instinct. The problems or threats have their origin and with the time can go being equal or better, that is why the question arises what has been the evolution that has taken the Social engineering between 1950 until 2017 and that consequences have been?

After having raised the problem, the revision is oriented toward the identification of social engineering techniques among which are phishing, scam, whaling, pharming, smishing, attack in person, among others, then analyzed as these have advanced in the time to reach the preventive measures, in pro to generate awareness in front of the proper management of the information that is generated daily. Finally, after an extensive tour bibliographical, concludes with a set of suggestions to avoid becoming the victim of social engineering.

Keywords:
DECEPTION, MANIPULATION, CRIMINALS, MALWARE, RAMSONWARE

GLOSARIO

ATAQUE-CIBERNETICO: Toda acción que busca atentar contra un sistema informático o redes computacionales, sea en beneficio propio o de terceros.

CIBER-DELINCUENTE: Aquellas personas que, con un conocimiento elevado en relación a la informática y ciencias de la computación, utilizan los ordenadores y redes para cometer delitos.

CRACKER: Entendido como un vandálico virtual que busca agredir sistemas, desentrañar password de software y códigos fuente o violentar patrones de licenciamiento.

CRYPTOLOCKER: Tipo de ransom fundamentado en la extorsión al usuario, donde se secuestra la información por medio de la encriptación para luego pedir un tipo de intercambio que puede ser monetario u otro.

HELP DESK: Ataque basado en la solicitud de ayuda o apoyo, donde la víctima es engañada para que revele información como accesos o viceversa.

INGENIERIA SOCIAL (IS): entendida como el arte de manipular al usuario para que realice actos que normalmente no haría, todo debido a lo débil que es el ser humano.

MALWARE: Software maligno que tiene la finalidad de causar daño a un sistema o fallas en su manejo, puede abarcar múltiples variantes, dependiendo para lo que haya sido programado.

PHISHING: Tipo de ingeniería social, la cual tiene la finalidad de llevar a cabo un engaño y lograr que el usuario otorgue información de modo fraudulento, las acciones más implementadas son: envío de correo con link de sitios web falso y recolectar usuarios y contraseñas.

RANSOMWARE: Software maligno cuya finalidad puede llegar a estar en bloquear sistemas y secuestrar la información por medio de la encriptación, para luego solicitar un tipo de pago como Bitcoins (este es uno de los más utilizados).

SPAM: Definido como mensaje no deseado enviados vía correo electrónico, el cual busca en algunos casos realizar desde infección con virus hasta un tipo de phishing y viceversa

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

1. INTRODUCCIÓN

La seguridad es demasiado a menudo solo una ilusión, que se vuelve peor aún, cuando la ingenuidad, ignorancia o credulidad entran en juego[1], la frase anterior redactada por Kevin Mitnick en su libro el Arte del Engaño, nos plantea de manifiesto la manera como algo que parece solido puede convertirse en lo más frágil del mundo.

Los sistemas informáticos se saben que no tienen un 100 % de seguridad plena, pero ello no implica que no tengamos uso de razón en muchas de las ocasiones, donde debido a la ingeniería social se obtienen datos de otra persona sin darse cuenta esta que los otorga, teniendo como base al artificio de usuarios para que buenamente realicen acciones como entrega de contraseñas, otorgamiento de permisos y otras actividades que normalmente no harían[2].

La ingeniería social como es conocida actualmente hace referencia a un arte o manera de actuar de determinadas personas, debido a que busca la manipulación del ser humano utilizando infinidad de técnicas y métodos[3]; es por ello que la indagación bibliográfica busca visibilizar desde un nivel global la manera cómo ha evolucionado la IS, tomando el antes y el después para analizar cómo se desarrollan y previenen los diferentes ataques que pueden llegar a afectar la seguridad informática.

Inicialmente para esta indagación se parte de analizar una situación problemática donde interviene tres elementos o factores: el ser humano, su manera de actuar y el medio por el cual se está actuando; estos se vuelven trascendentales a la hora de la gestión de un producto o servicio, que para el caso actual es la información. Según como se ha ido adelantando en la revisión bibliográfica, se han encontrado técnicas dentro del rango de tiempo elegido y como se han desarrollado en su debido momento, haciendo pensar que es algo irónico que suceda, pero la realidad es que ha sucedido y sigue sucediendo.

La presente propuesta surge de una situación la cual se plantea en una pregunta, luego de ello arranca una revisión bibliográfica intensiva identificando técnicas y casos de la vida real, donde la ingeniería social ha sido el eje principal del problema, pasando luego a proponer una serie de medidas preventivas en pro de concientizar al usuario para que no se vuelva una víctima más. "La clave no está tanto en lo que se dice sino en cómo se dice” Brian Leggett

---

[1] MITNIK Kevin, El arte de engaño, 2001 [Online], disponible en http://www.seaceptanideas.com/biblio/El_Arte_del_Enga%C3%B1o.pdf

[2] MORALES, José André Ph.D., Ingeniería Social, Cibercamp, 2014.

[3] GOMEZ, Álvaro. Enciclopedia de la Seguridad Informática, Ingeniería Social, 2ª Edición, México DF, ALFAOMEGA GRUPO EDITOR S.A, 2014, 134p.

2. DEFINICIÓN DEL PROBLEMA

1.1 DESCRIPCIÓN DEL PROBLEMA

Si conocemos el origen, podemos interpretar el presente y llegar a predecir el futuro. Desde la construcción de la famosa “máquina Mark 1 considerada como el primer ordenador comercial, se han venido gestando una serie de transformaciones, donde en muchos casos se introdujeron nuevos computadores unos mejorando lo que desarrollaban los otros”[4], todo ello buscando dar solución a un problema que podría ser matemático o de otra índole, llegando a la construcción de soluciones de comunicación como “la red ARPANET el 4 de octubre de 1957 que dio origen al internet”[5].

Pero los avances dieron inicio a un problema. Inicialmente con el teléfono se adelantaban bromas o suplantación por medio de la voz, a su vez esta permitía la manipulación de personas aplicando la psicología para persuadir; Todo ello ha sido el punto de partida para el surgir de la ingeniería social y sus variadas técnicas, que a simple vista pueden ser insignificantes pero su implicación genera un gran riesgo para usuarios.

Al momento de ejecutar un ciberataque por medio de ingeniería social se pueden encontrar múltiples escenarios, donde cada uno de ellos compromete cierto nivel de seguridad y de información, algunos de los más utilizados y conocidos son:[6]

- Sitios web: Conforme como lo menciona Verizon en su reporte de investigación emitido en 2014, "sitios web altamente estratégicos son utilizados para la distribución de malware correspondiente a un 20 % de los ataques de espionaje".

- Correo electrónico: Gracias al correo electrónico los ciberdelincuentes pueden conseguir un procedimiento eficaz por medio del uso de phishing y phishing selectivo, ya que como se menciona en el reporte de Verizon, "El 18 % de los usuarios acceden a enlaces que van inmersos en mensajes de

[4] Escola Tècnica Superior d’Enginyeria Informàtica, Un Viaje a la Historia de la Informática, La Génesis del Ordenador Moderno, España, EDITORIAL UNIVERSITAT POLITÈCNICA DE VALÈNCIA, 2016, 15p, disponible en: http://museo.inf.upv.es/wp-content/uploads/2016/12/Un%20viaje%20a%20la%20historia%20de%20la%20inform%C3%A1tica.pdf

[5] Escola Tècnica Superior d’Enginyeria Informàtica, Un Viaje a la Historia de la Informática, Apuntes sobre los Orígenes de Internet, España, EDITORIAL UNIVERSITAT POLITÈCNICA DE VALÈNCIA, 2016, 71p.

[6] CHARLES McFarland, Ataques al sistema operativo humano, Intel Security, [En línea], 2015. Disponible en: <http://www.ebankingnews.com/wp-content/uploads/2015/02/Informe-Ataques-al-sistema-operativo-humano_feb_2015.pdf >.

phishing".

- Telefonía: Medio muy estimado para la reventa de información y el desarrollo de estafas.

- Cara a cara: Donde el atacante encara presencialmente a un usuario y procede a engañarlo o ejerce presión para que otorgue información confidencial.

- Servicio postal: Aunque no es un muy utilizado en la actualidad, se pueden llegar a presentar casos de ingeniería social por este medio.

En un reporte presentado por la multinacional ESET para el año 2015 nos deja ver casos de ingeniería social como lo son: “La estafa nigeriana (o estafa 419), scams en relación a muerte de personalidades y noticias ficticias angustiosas de redes sociales” [7], todo ello ha sido el reflejo de lo que Kevin Mitnik llama el arte del engaño.

Un ejemplo muy claro de lo que puede llegar a pasar por no manejar correctamente la información es el siguiente:

Llamada telefónica:

Cliente: ¿Hola con quien hablo?

Ciberdelincuente: Buenos días, hablas con Pedro del área de sistemas.

Cliente: ¿Pedro? del área de sistemas?

Ciberdelincuente: ¡Sí! (expresando seguridad en la voz) presentas algún inconveniente con tu usuario? acá me figura un error.

Cliente: Pues no veo ningún problema.

Ciberdelincuente: Puede que sea una falla nuestra, a ver, dime tu ID de usuarios.

Cliente: Si... es "klopez"

[7] PAGNOTTA Sabrina, Las 5 historias de Ingeniería Social más ridículas de los últimos tiempos, ESET, [En línea], 2015. Disponible en: https://www.welivesecurity.com/la-es/2015/12/01/historias-de-ingenieria-social-ridiculas/

Ciberdelincuente: ¿Seguro? voy a buscarlo en mi listado de users... ok. Si está ¿dime tu contraseña actual para realizar un cambio por otra más segura?

Cliente: Si... es "andres20"

Ciberdelincuente: Muchas gracias. Que estés bien, hasta pronto.

Tomado de (Ingeniería Social: Hacking Psicológico, OWASP).

Algo como una llamada telefónica puede poner en riesgo toda una infraestructura de la red, creemos saberlo todo, pero a la hora de la verdad somos falibles en todo sentido. El ejemplo anterior es uno de muchos utilizados en ingeniería social. ¿Cómo eran los ataques antes y cómo son ahora?

1.2 FORMULACIÓN DEL PROBLEMA

¿Cuál ha sido la evolución que ha tenido la ingeniería social entre 1950 hasta 2017 y como se puede evitar ser víctima?

2. JUSTIFICACIÓN

Al llevar a cabo el actual trabajo se pretende dar a entender la manera como se desarrolla la ingeniería social, las técnicas que utiliza para ejecutar diferentes ataques y como pueden ser prevenidas; analizándolas desde un contexto evolutivo para llegar a brindar un conjunto de recomendaciones buscando evitar ser víctimas o convertirnos en ciber-delincuentes. Por tal motivo se realiza un estudio bibliográfico partiendo del año 1950 hasta llegar al 2017.

El usuario de ordenador estará en capacidad de reconocer si una acción determinada es o no ingeniería social aplicada, partiendo de un reconocimiento tanto psicológico como informático; Las personas por naturaleza son lo más frágil de la seguridad informática, teniendo en cuenta que somos predecibles con la información que tenemos y manejamos. Muchos de los ataques cibernéticos ocurridos 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 conocer las técnicas y cómo prevenirlas es de vital importancia al momento de gestionar políticas de seguridad informática.

Aunque hay múltiples medios para el desarrollo de ataques de ingeniería social, el más utilizado es el correo electrónico llamado spam, donde diariamente se reciben emails como procesos judiciales, deudas de impuestos, entre otros; Todo ello buscando siempre que descarguemos archivos maliciosos y luego de modo remoto ejecutar robos atacando sistemas.

¿Cómo podemos llegar a convertirnos en víctimas? en algunas ocasiones un usuario recibe un correo indicándole sobre una situación que debería resolver y por ignorancia o presión, descarga un fichero y/o accede a una página web por medio de un link, lo que conlleva a que todo su sistema e información quede expuesto; no solo con un e-mail podemos llegar a estar en riesgo, también con otras técnicas como Phishing, acceso no autorizado, USB tentadoras, entre otras.

Teniendo en cuenta que un incidente puede ocurrir en cualquier momento y de diferente tipo, se pretende adelantar la presente monografía buscando llevar a cabo una revisión histórica del antes y el ahora de la ingeniería social, la cual permita brindar las herramientas para que el usuario asuma una actitud más responsable con el uso de la información.

3. ALCANCE

Llevar a cabo una revisión bibliográfica de diferentes técnicas de ingeniería social desarrolladas en un contexto del antes y el ahora entre 1950 - 2017, determinando las implicaciones que pueden generar el ser víctima, por lo cual se exploran ataques y su prevención; ya que como se sabe en informática no hay nada 100% seguro, habrá que estar en constante actualización.

Resultado de ello se debe replantear la importancia de una correcta valoración de la información que día a día se genera y maneja, teniendo presente el mundo interconectado en el cual vivimos, adoptando políticas acertadas de seguridad.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Ejecutar un análisis bibliográfico entre los años 1950 y 2017 donde se adelante un reconocimiento de la evolución que ha tenido la ingeniería social y las medidas preventivas que eviten consecuencias del lado de la víctima.

4.2 OBJETIVOS ESPECÍFICOS

Explorar referentes teóricos sobre ataques de ingeniería social entre los años 1950 y 2017.

Analizar los avances que han tenido las técnicas de ingeniería social desde sus orígenes hasta la actualidad.

Brindar medidas preventivas que sirvan para la educación de diferentes usuarios, en búsqueda de que no se conviertan en víctimas de ataques de ingeniería social.

5. MARCO TEÓRICO

Teniendo en cuenta que el análisis del actual trabajo busca identificar la manera como se han desarrollado diferentes técnicas de ingeniería social con el transcurrir de los años, es necesario entender el funcionamiento en cada una de sus etapas, del mismo modo como lo expuso Kevin Mitnik en su libro “El arte del Engaño”; visibilizando múltiples escenarios donde el ser humano se convierte en lo más frágil de la seguridad informática.

El ser humano y el ordenador han establecido a lo largo del tiempo una relación tanto fuerte como débil, la cual ha sido motivo de estudio en la ingeniería social por diferentes estamentos de educación superior a nivel nacional y el mundo, llegando a ser algunas de tipo monografía y otras investigativas con enfoques muy diferentes; pero lograr identificar los factores que intervienen en el problema nos lleva a revisar como la psicología interviene y gracias a ella se persuade al usuario de ordenador, tal como lo trata el estudiante de Ingeniería en Informática Sergio Argos en su proyecto de grado “Ingeniería social: Psicología aplicada a la seguridad informática”[8].

Sin lugar a duda, cualquier persona puede llegar a convertirse en ciber-delincuente por medio de actuar y de influir en otro; las anécdotas y los casos de la vida real dados a conocer en el libro el arte de la intrusión por Kevin Mitnik son el vivo ejemplo de lo que ocurre y puede llegar a ocurrir.

Todos los estudios revisados en los antecedentes del problema nos dejan ver como se han tratado los ataques desde una perspectiva general y puntual, pero no se ha analizado toda la evolución y adaptación que estos han tenido.

[8] ARCOS, Sergio. Ingeniería Social: Psicología aplicada a la seguridad informática. Trabajo de grado Ingeniería en Informática. Barcelona, España: Universitat Politécnica de Catalunya. Departamento de Ingeniería de Servicios y Sistemas de Información, 2011. 22p. Disponible en: https://upcommons.upc.edu/handle/2099.1/12289

6. MARCO LEGAL

Nacional

Ley 1273 de 2009*, Congreso de la Republica de Colombia*

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. En este se dictamina lo relacionado al acceso no autorizado o al salirse de lo acordado tanto en todo o en parte a sistema informático, lo que hace que se tipifique un delito.

Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. En este se tipifica lo relacionado con diseño, desarrollo, transferencia, ventas, ejecución, programación y el envío de sitios web o ventanas emergentes sin estar debidamente facultado, lo que hace que se incurra en un delito teniendo en cuenta que también afecta la alteración del servidor de resolución de nombres de dominio.

Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. En este el que transfiera cualquier activo con el ánimo de lucro y valiéndose de manipulación informática no consentida incurrirá en un delito. [9]

Ley Estatutaria 1581 de 2012, En esta de dictaminan todas las disposiciones para la correcta protección de datos personales.[10]

Ley No 1928 de 2018. *Congreso de la Republica de Colombia*

Ley en la cual se realiza la aprobación del <<Convenio sobre la ciberdelincuencia>>, adoptado el 23 de noviembre de 2001, en BUDAPEST.

Artículo 2. ACCESO ILÍCITO: Cada una de las partes deberá adoptar las medidas legislativas o de otro tipo para la tipificación como delito el acceso deliberado e ilegitimo a un sistema informático tanto en su totalidad o parte de este.

[9] CONGRESO DE LA REPUBLICA, Ley 1273 de 2009, Bogotá, Colombia, Disponible en http://acueductopopayan.com.co/wp-content/uploads/2012/08/ley-1273-2009.pdf

[10] CONGRESO DE LA REPUBLICA, Ley Estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, 2013, Disponible en: https://www.sisben.gov.co/Documents/Informaci%C3%B3n/Leyes/LEY%20TRATAMIENTO%20DE%20DATOS%20-%20LEY%201581%20DE%202012.pdf

Donde se puede exigir que dicho delito se cometa infringiendo medidas de seguridad.

Artículo 3. INTERCEPTACIÓN ILÍCITA: Cada una de las partes tomará las medidas legislativas para la tipificación como delito la interceptación ilegitima y deliberada de la información utilizando diferentes medios informáticos.

Artículo 6. ABUSO DE LOS DISPOSITIVOS: Las partes adoptarán las medidas legislativas o de otro tipo para la tipificación como delitos: la producción, venta, obtención para utilización, importar, difundir u otra forma lo siguiente:

1. Un dispositivo incluyendo un programa para la comisión de cualquier delito previsto en los anteriores artículos 2 a 5.

2. Contraseñas, códigos o datos para el acceso a un sistema informático en parte o totalidad con el fin de tipificar cualquier delito contemplado en los artículos 2 a 5.

Artículo 7. FALSIFICACIÓN INFORMÁTICA: Las partes adoptaran medidas legislativas u otras para tipificar como delito la introducción, alteración, borrado o supresión de datos informáticos dando lugar a datos no auténticos.

Artículo 8. FRAUDE INFORMÁTICO: Medidas legislativas o de otro tipo serán adoptadas por las partes, resultado de la necesidad para tipificar como delito los actos ilegítimos y deliberados que provoquen un perjuicio patrimonial a otras personas mediante borrado, alteración, supresión y cualquier interferencia en el funcionamiento de un sistema informático.[11]

Europeo

Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016. (29) A fin de alcanzar y mantener un elevado nivel de seguridad tanto de las redes como de sistemas informáticos los Estados miembro deben disponer de una estrategia nacional de seguridad en relación a redes y sistemas de información.[12]

[11] CONGRESO DE LA REPUBLICA, Ley No 1928 de 2018, Por medio de la cual se aprueba el <<convenio sobre la ciberdelincuencia>>, adoptado el 23 de noviembre de 2001, en BUDAPEST, Disponible en: http://es.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf

[12] PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA, Directiva (UE) 2016/1148, de 6 de Julio de 2016, Disponible en: https://www.boe.es/doue/2016/194/L00001-00030.pdf

7. LA PERSUASIÓN Y LA INFLUENCIA

La RAE define a la persuasión como incitar, desplazar, forzar a alguna persona a que realice algo haciéndole creer con razón. Dentro de la psicología se entiende como un proceso por el cual una misiva se dota de razonamientos soportados, con el fin de cambiar la actitud de un usuario, gestando que adelante cosas que con otro uso de razón no haría.[13]

Al ejecutar la persuasión la cual se apoya en la influencia que es entendida como la obtención de una ventaja, favor o beneficio por parte de una persona basándose en el poder o autoridad; dentro de esta se distinguen seis principios los cuales son definidos por Robert Cialdini como:

a) Reciprocidad: Es la sensación o adeudamiento afectivo que se contrae cuando apreciamos que una persona nos brinda alguna cosa ya sea servicio o bien. "Si te doy mi apoyo, solo queda esperar el transcurso del tiempo para que lo retorne cuando lo pida".

b) Escasez: Aquello que se percibe como escaso se blinda de un valor exclusivo volviéndolo único lo que hace que "Si alguien siente que una persona da algo a él en modo exclusivo (Una relación que otorga unión), quede abierto un canal de influencia".

c) Autoridad: Donde la otra persona transmite autoridad la cual es percibida y transformada en influencia.

d) Simpatía: Una persona con un nivel de bienestar considerable, puede llegar a ser más influenciable que otra.

e) Coherencia: Indicar algo y hacerlo.

f) Validación Social: Busca que las personas por tendencia hagan lo que hace la mayoría, validándose la conducta socialmente.[14]

El conocer a que se refiere la persuasión, las herramientas que usa y su finalidad, nos permite ir adentrándonos en el conocimiento de cómo esta es aplicada en la ingeniería social para llevar a cabo múltiples ataques, tomando como punto de entrada la persona que es el escalón más frágil en la seguridad informática.

---

[13] CASTILLERO M. Oscar, Persuasión: definición y elementos del arte de convencer, Psicología Social y Relaciones personales, 2016, Disponible en: https://psicologiaymente.com/social/persuasion-definicion-elementos-convencer

[14] ESCUDERO C. JAVIER, Estrategias para persuadir, ISSN 1138-9702, Nº. 117, 2007, págs. 83-94, disponible en: http://www.infoservi.com/infoservi/descargas/45_Estrategias_Para_Persuadir.pdf

8. EL GÉNESIS DE LA INGENIERÍA SOCIAL

La ingeniería social es usada en política con varios sentidos, uno relacionado a esfuerzos para la influencia de actitudes, relación o acciones sociales sobre la población de un país o región y el otro es implementado en programas de transformaciones sociales.

En sus inicios las empresas utilizaban el termino ingeniería social para referirse a la persona que tenía función de mediador en la resolución de conflictos con intermediación racional entre el capital y el trabajo. Por ello se tenía que contar con habilidades sociales. La expresión inició en un ensayo creado por el empresario holandés J.C. Van Marken, quien también ejercía como filántropo en 1894 y difundido por Émile Cheysson, recibiendo el mayor impulso en EE.UU por medio del libro "Social Engineering" de W.H. Tolman, quien ayudaba a los pobres en aquella época.[15]

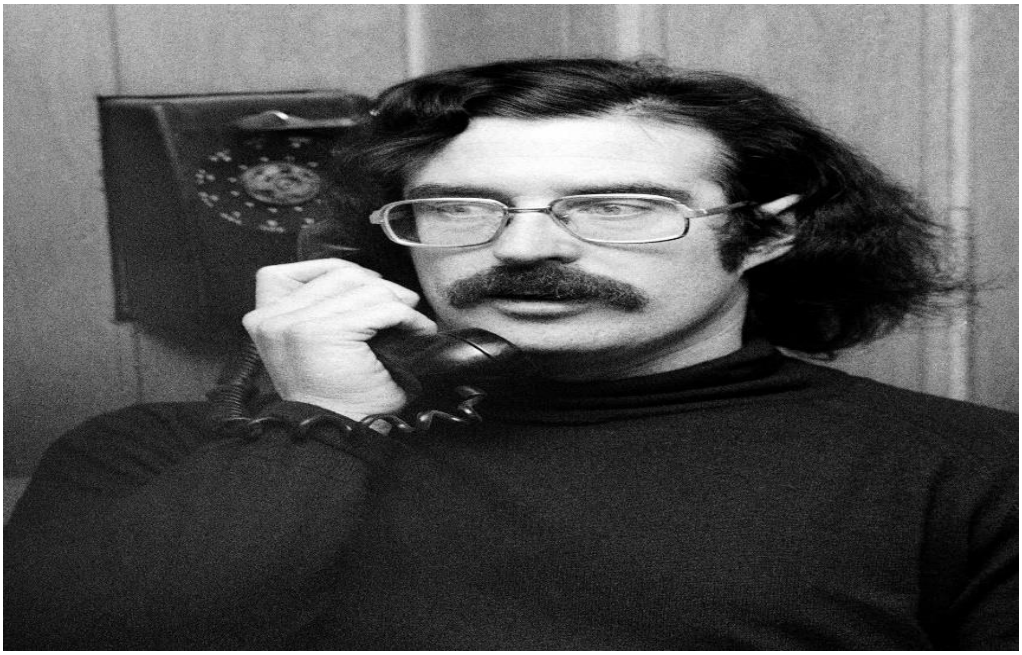
El termino tiene sus orígenes en pensadores liberales y sus conceptos filantrópicos hacia mediados del siglo XIX, cayendo en desuso para las décadas de 1930 y 1940.

El termino ingeniería social sufre una reintroducción por parte de Karl Popper en 1945 donde puede llegar a ser método o técnica para el logro de una gran multiplicidad de resultados, es decir se deja de lado como un instrumento para la resolución de conflictos sociales y se transforma en una manipulación de personas. En algunos casos las propagandas o campañas político religiosas se convierten en ingeniería social ya que buscan un comportamiento especifico de la población.[16]

En los inicios los hackers eran conocidos como phreakers (phone + hack + freak). Aquellos que se preocupaban por saber el funcionamiento de la telefonía y el manejo de sistemas de comunicación incluyendo la tecnología y las compañías telefónicas.

[15] LEDESMA, Cristina. LEDESMA, Ana & PASCALE Maricarmen, Ingeniería social - El hackeo al ser humano. Un enfoque holístico, 2014, disponible en: http://www.magazcitum.com.mx/?p=2747
[16] LEDESMA. cit. p.1.

Figura 1. John Draper y el origen de los Phreaks[17]



En mucho de los casos no se logra identificar que se está siendo víctima de ingeniería social, se escucha acerca de delitos informáticos como robo de información, ataques con virus y algunas técnicas utilizadas por personal de sistemas para engañar, muy pocos conocen que corresponde a ingeniería social la cual se puede entender como el manejo sabio de la vocación nativa de las personas a confiar (icde.org.co), o también como doctrina que consta en obtener datos a otro usuario sin que él sepa que está brindando información delicada (icde.org.co) y artificio para que personas realicen acciones que no harían con un uso de razón normal. (carole fennelly, the human side of computer security, sunworld, July 1999).[18]

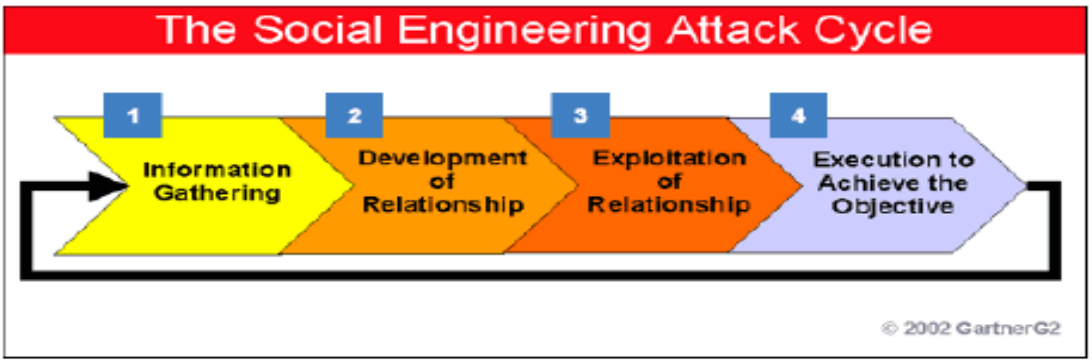
[17] JORGE M. (2016) John Draper, unos de los primero Phreaks. [Figura]. Recuperado de https://es.gizmodo.com/pioneros-de-la-ingenieria-social-el-hacker-ciego-que-p-1789268307

[18] MORALES, José André Ph.D., Ingeniería Social, Cibercamp, 2014, disponible en https://cybercamp.es/cybercamp2014/attachments/multimedia/CyberCamp_IngenieriaSocial.pdf

9. FUNCIONAMIENTO DE LA INGENIERÍA SOCIAL

Las arremetidas de la ingeniería social pueden llegar a ser de diverso tipo, pero todo ello tiene una estructura funcional básica similar, la cual se ejecuta en ciclos y estos pueden ser visualizados en la figura 2:

Figura 2. Descripción pasos The Social Enginnering Attack Cycle[19]



Cada uno de los pasos mencionados son explicados en la Tabla 1.

Tabla 1: Pasos utilizados dentro de la ingeniería social[20]

PASOS UTILIZADOS DENTRO DE LA INGENIERIA SOCIAL	
Investigación	Se realiza una recolección de información, como informes, material, datos de la víctima, todo ello buscando construir un anzuelo exitoso y determinar la mejor forma de acercarse al objetivo construyendo relaciones.
Anzuelo	Se da inicio a la farsa, construyendo un grado de intimidad gracias a la colaboración con el objetivo y se toma control de la interacción.
Desarrollar rapport	Basado en los datos conseguidos anteriormente, se

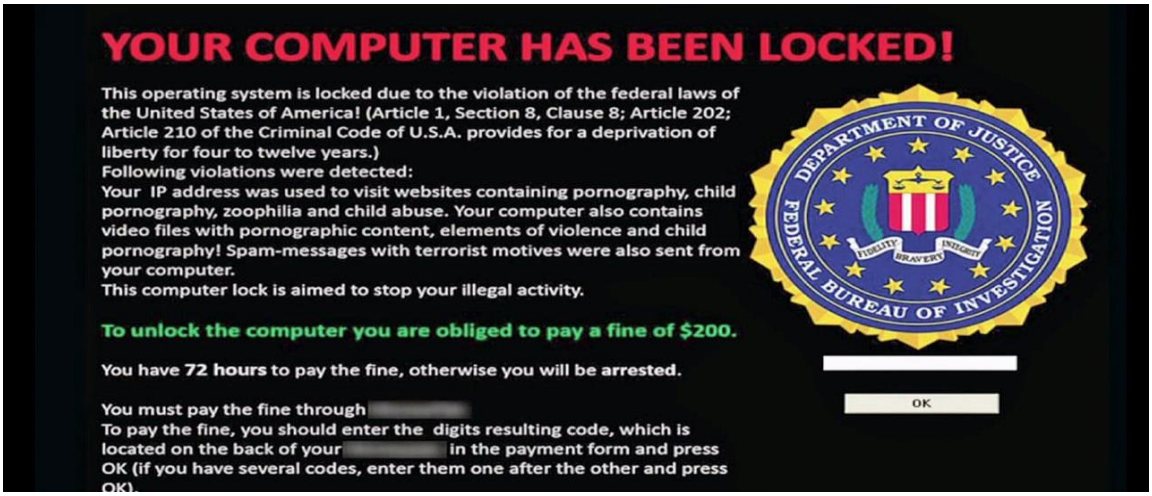
[19] MORALES J. Ph.D (2014) Ciclo de ataque de Ingeniería Social. [Figura]. Recuperado de: https://cybercamp.es/cybercamp2014/attachments/multimedia/CyberCamp_IngenieriaSocial.pdf

[20] MITNIK Kevin, El arte de engaño, 2001 [En línea], disponible en http://www.seaceptanideas.com/biblio/El_Arte_del_Enga%C3%B1o.pdf

y credibilidad	cambian las identidades, se le exige a la víctima, se le puede pedir apoyo o hacer uso de la autoridad.
Aprovechar confianza	Se consulta o logra que te pregunten con tal de extraer información y mantener las cosas con el suficiente tiempo, se sostiene 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 repite el ciclo con tal de lograr el objetivo, se provee al usuario de las razones para guardar silencio.
Lanzar Ataque a Sistema	Este es el paso final 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.

Dentro del software malicioso que se pueden implementar en el final del ciclo de vida de la ingeniería social están de tipo ransomware, cryptolocker y/o cualquier otro troyano, lo cual puede llegar a secuestrar información valiosa; el siguiente es un ejemplo que muestra el momento de ejecución y se puede ver en la Figura 3.

Figura 3. Ransomware una amenaza creciente[21]



[21] PYMNTS, Ransomware una amenaza creciente. (2016), [Figura]. Recuperado de: https://www.pymnts.com/news/security-and-risk/2016/why-the-fbi-thinks-ransomware-is-a-growing-threat/

Modus Operandi

Un mensaje altamente verídico, fidedignas sean las fuentes y se confíe el usuario, esto le permitirá al atacante concretar con éxito la recolección de información o la expansión de malware, todo lo anterior genera mayores posibilidades de culminar la preparación del engaño en particular y lograr la aplicabilidad de la ingeniería social.[22]

Muchas personas tienen una idea errónea sobe ciberataques pensando que solo se necesitan herramientas y tecnología avanzada de hackeo para poder irrumpir en las computadoras, equipos móviles o cuentas de los usuarios. Esto queda entredicho así de simple. Los ciber-atacantes han identificado la manera más fácil de robar tu información o de hackear tu PC usando las palabras para engañarte.[23]

Una de las trampas preferidas al momento de aplicar la ingeniería social está relacionada con la lectura en frio. Entre tanto, el atacante detalla las señales no verbales que la víctima lanza y entonces, libera algo que haga razonar. [24] La manera como se puede ser engañado es tan sencilla como se explica a continuación en el siguiente ejemplo:

> Cuando un atacante se acerca a la entrada, donde anteriormente le había visualizado a los empleados sus placas, se dirigió a donde se encontraba el guardia del mostrador y le dice: ¡Eh! ¿Has visto a Cherry? me está debiendo 20 dólares del juego y requiero el dinero para merienda en el descanso.
>
> Recordando aquel hecho exclama: ¡Uff! el guardia dijo ¿Y por qué quieres adquirir comida? y suelta una sonrisa entre dientes, pero le causa sospecha. Ligeramente deje escapar: He quedado con un bomboncito para comer, tío. Está muy buena. (Un comentario que tiende a distraer a los viejos, a los que viven con mamá y los que guardan línea) ¿qué voy hacer? el guardia le contesta: Lo entiendes porque Cherry se ha ido por el resto de la semana, ¡Será...!, exclamé. El guardia le hace un gesto a Whurley para preguntarle repentinamente si estaba enamorado. El guarda me dio 50

[22] BARRERA IBáÑEZ Silvia, La Ingeniería Social y Cibercrimen, 2015, disponible en http://www.cajarural.com/rurales/blog/2015/ingenieria_social.pdf

[23] TORRES Alissa, Ingeniería Social, Securing the human SANS, 2014.

[24] MITNIK Kevin & SIMON William, El arte de la Intrusión, Alfa Omega Editor, ISBN 978-970-15-1260-9, 2007, disponible en https://radiosyculturalibre.com.ar/compartir/biblioteca/INFOSEC/Mitnick%20Kevin%20-%20El%20Arte%20De%20La%20Intrusion.PDF

> dólares. Me dijo que con 20 no se adquiere nada decente y que, obviamente, tenía que ser yo el que pagara.[25]

El tener la tecnología más sofisticada como, corta fuegos, IDS (Sistema de Detección de Intrusos), lectores biométricos u otro no es garantía de seguridad. Solo se necesitará un llamado a un empleado que se encuentre desprevenido y acceder, teniendo todo en sus manos. Como se vio en el anterior ejemplo; el ser humano es el eslabón más frágil de los sistemas. No le gusta decir que no, siempre quiere ayudar a otros.[26]

Las agresiones con ingeniería social llegan a tener éxito en el momento en que las personas se vuelven tontas o ignorantes sobre verdaderas prácticas de seguridad informática, pasando a ser solo una alucinación, convertida en algo peor cuando, la ignorancia, credulidad o ingenuidad entran en acción. Muchos profesionales de la tecnología (IT) tiene la certeza errónea que han convertido sus empresas inmunes a ataques porque implementan la seguridad estándar de productos como cortafuegos, IDS o autenticación.[27]

Entre las finalidades de la ingeniería social encontramos:

a) Los usuarios reciben un mensaje tipo spam donde son tentados a adelantar una acción con la finalidad de vulnerar o dañar un sistema a través de un enlace a página web, archivo adjunto o video.

b) Los usuarios terminan otorgando información necesaria gracias a datos obtenidos ya sea por scam o phishing, para luego el atacante realizar una acción fraudulenta.[28]

Los motivadores Utilizados por los Ingenieros Sociales para adelantar ataques son[29]:

- Reciprocidad: Creer que se adeuda un servicio a quien realizó algo por nosotros.

---

[25] ibid., p. 304
[26] MORALES. Óp. cit., p. 9.
[27] MITNIK Kevin, El arte de engaño, 2001, disponible en http://www.seaceptanideas.com/biblio/El_Arte_del_Enga%C3%B1o.pdf
[28] BORGHELLO Cristian, El arma infalible: La ingeniería Social, Technical & Educational Manager de ESET Para Latinoamérica, disponible en http://www.eset-la.com/pdf/prensa/informe/arma_infalible_ingenieria_social.pdf
[29] SHACKLEFORD, Dave. Pruebas de penetración en ingeniería social: cuatro técnicas efectivas, [En línea], TechTarget. 2012, Disponible en: https://searchdatacenter.techtarget.com/es/consejo/Pruebas-de-penetracion-en-ingenieria-social-cuatro-tecnicas-efectivas

- Orientación social: Se busca a personas que nos digan cómo se debe proceder.

- Consistencia/compromiso: Hábitos que son creados a base de patrones de conducta.

- Aceptación: Buscar encajar con aquellas personas que nos gustan, donde nos persuaden con mayor facilidad.

- Autoridad: Nos gusta recibir mandatos y requerimientos de personas que expresan autoridad.

- Tentación: Nos motiva algo exclusivo o limitado por perseguir.

Descubrir y detener ataques de ingeniería social

Para ejercer la defensa contra ataques de ingeniería social una forma fácil y simple es usar el sentido común. Si tienes sospechas de algo o la impresión que da no es buena, puede ser un ataque. Entre los indicadores comunes de se incluyen:

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

- Si piden información que no deberían tener o que ya tendrían que conocer, 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.[30]

Entre los métodos de comunicación que utiliza un ingeniero social encontramos:

- persona a persona

- celular

- correo electrónico

[30] TORRES Alissa, cit., P. 2

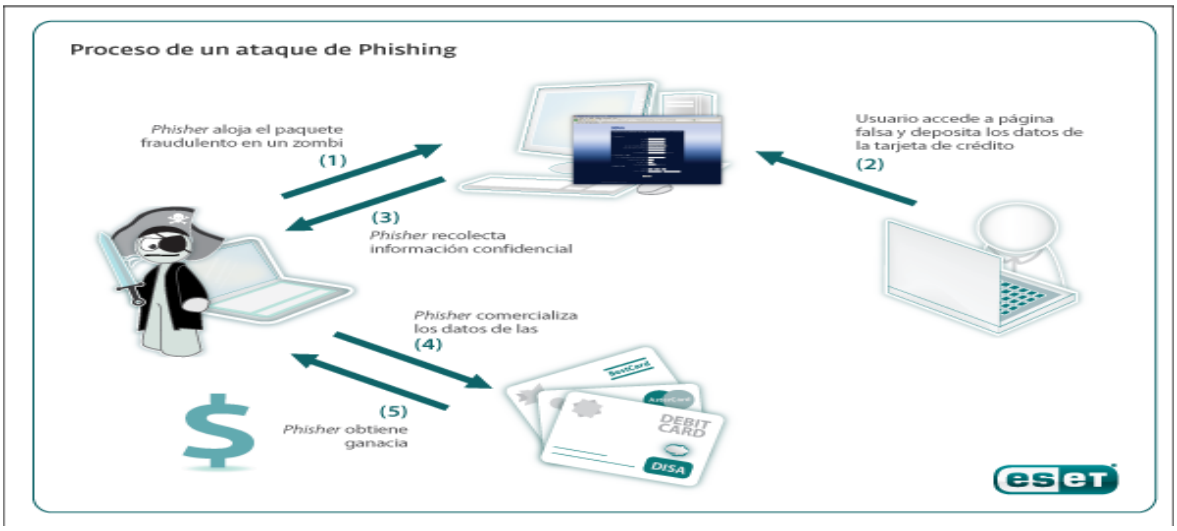
- MSN
- sitio web

9.1 TÉCNICAS DE INGENIERÍA SOCIAL

9.1.1 Phishing

Técnica de ingeniería social en la que los criminales cibernéticos buscan engañarte para adelantar una acción. Muchos de estos ataques comienzan con el envío de un correo electrónico pretendiendo ser alguien o algo que se conoce o es confiable, como tu banco, amistad o tiendas en línea favoritas. Estos mensajes de E-mail te motivan a realizar algún evento como hacer clic en un enlace, abrir un archivo adjunto o responder un mensaje. Los delincuentes cibernéticos crean estos correos electrónicos a modo de que parezca convincente, enviándolos a miles de usuarios a nivel mundial.[31] El funcionamiento de este tipo de ataque lo podemos ver en la Figura 4:

Figura 4, Proceso de un ataque de Phishing[32]



[31] DANHIEUX Pieter, Phishing por correo electrónico, Securing the human SANS, 2013, disponible en https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201302_sp.pdf

[32] MORALES J. Ph.D (2014) Proceso de un ataque de Phishing. [Figura]. Recuperado de: https://cybercamp.es/cybercamp2014/attachments/multimedia/CyberCamp_IngenieriaSocial.pdf

Como protegerse de phishing:

Para gozar de 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.[33]

9.1.2 Whaling

Conocido como whaling phishing, es un tipo específico de ataque que se dirige a empleados con un alto perfil, como los CEO, buscando robar información, además si una cuenta de correo electrónico de la administración llega a estar comprometida, luego puede ser explotada para ataques contra los empleados o incluso fuera de la organización.[34]

9.1.3 Spear-Phishing

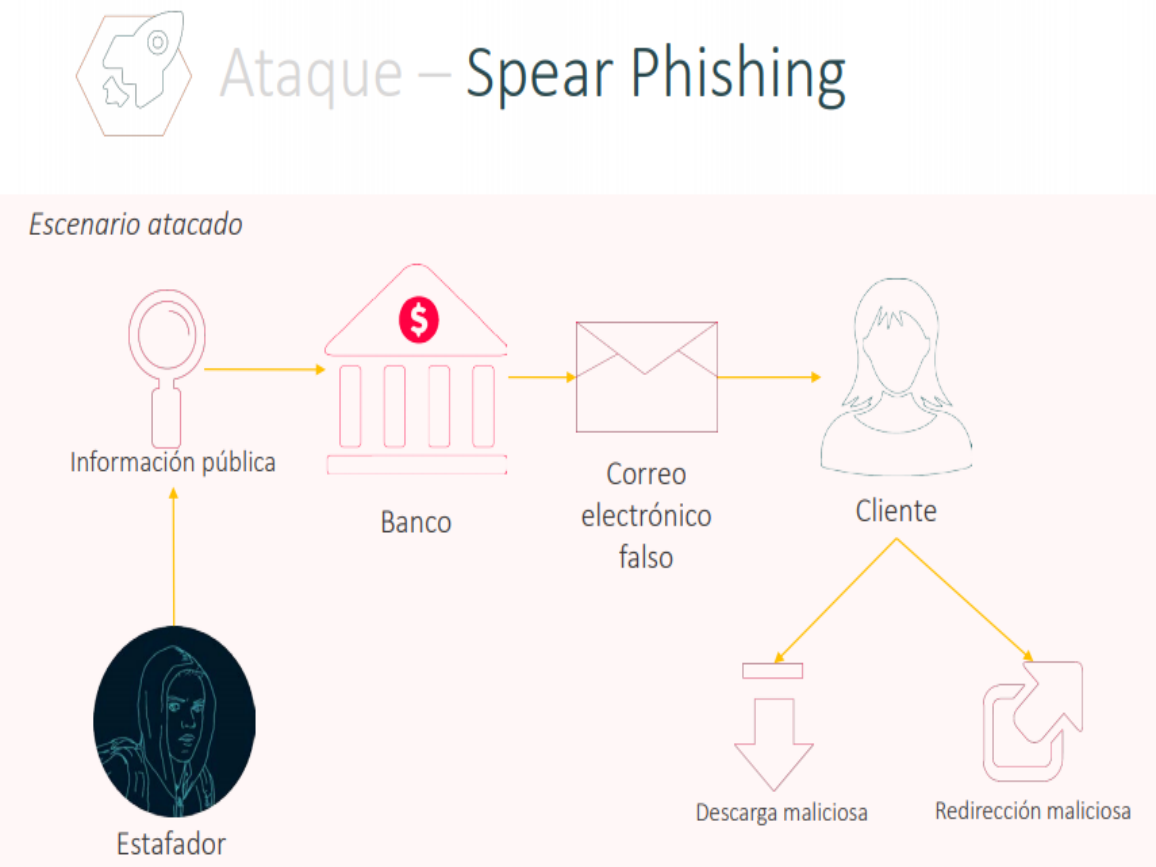
Conocida como estafa de correo electrónico dirigida a personas, organizaciones o empresas especificas donde aparte de buscar robar información pueden tratar de instalar malware en el computador de la víctima. La mejor forma para protegernos es la educación, donde estemos consientes de la responsabilidad del correcto manejo a la información que nos llega por e-mail.[35] El proceso básico de desarrollo de un Spear-Phishing, se puede visualizar en la figura 5.

[33] LUQUE José, Qué es el phishing y cómo protegerse, ASOCIAT, 2005, Disponible en: http://seguridad.internautas.org/html/451.html

[34] Royal Danish Defence College. Social Vulnerability & Assessment Framework - A Study on Social Engineering 2.0, Copenhagen Dinamarca, Dennis Hansen Editores, 2017, 67-69pp.

[35] KARPERSKY LAB. ¡Que es el spear phishing?, 2017, Disponible en: https://latam.kaspersky.com/resource-center/definitions/spear-phishing

Figura 5, Ataque – Spear Phishing[36]



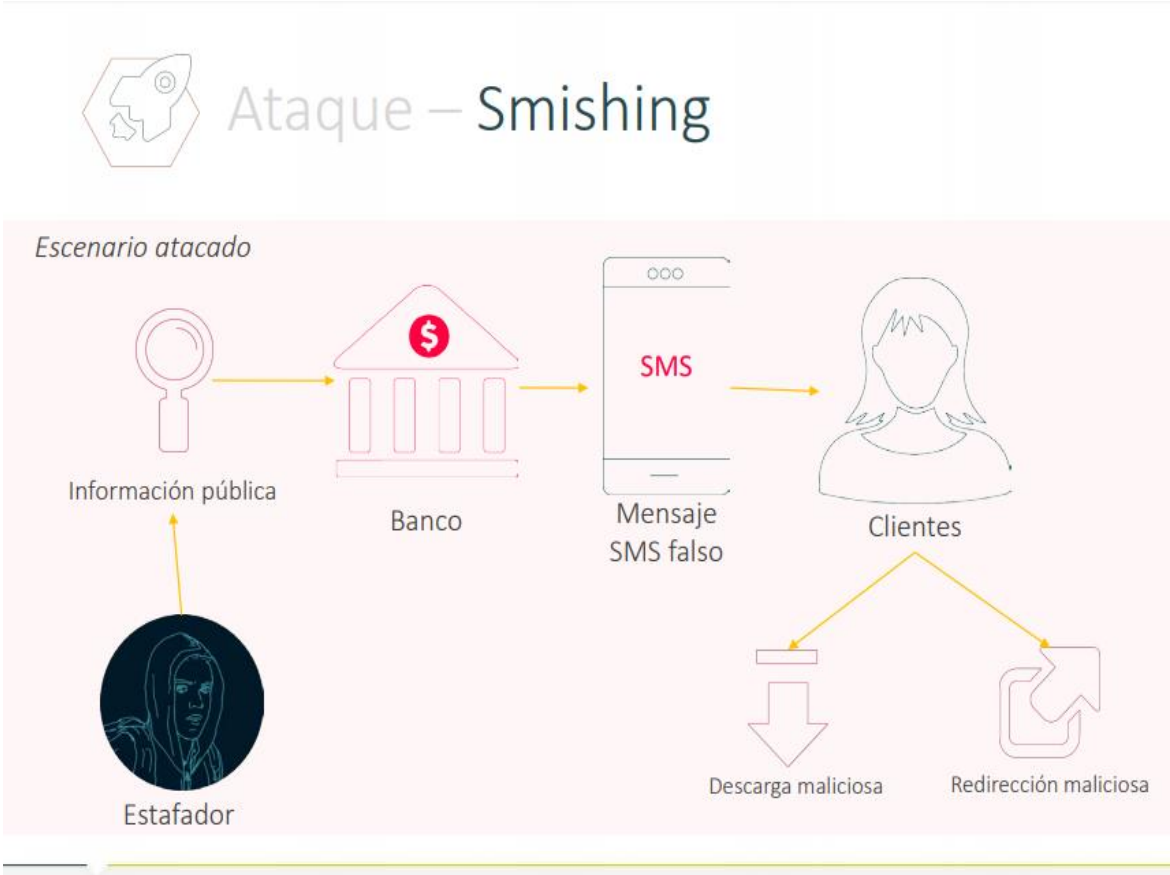
9.1.4 Smishing

Forma de phishing mediante el cual se intenta conseguir información privada a través de mensaje de texto SMS o número de teléfono. Los atacantes buscan datos desde contraseñas hasta información de tarjetas débito y crédito, de igual forma también pueden recibirse links con la alerta que deben abrirse o acarreará problemas.[37] Los pasos de un ataque smishing se detallan en la figura 6.

[36] MARINO DODGE, Juan. Ataque - Spear Phishing. En: Conferencia Fraude Electrónico [Figura]. Memorias. Bogotá D.C., 2017. p. 24-28 http://acis.org.co/archivos/Conferencias/2017/Conferencia0211.pdf

[37] SYMANTEC, ¿Qué es el smishing?, 2017, NORTON COLOMBIA, Disponible en: https://co.norton.com/internetsecurity-emerging-threats-what-is-smishing.html

Figura 6, Ataque – Smishing[38]



9.1.5 Help Desk

Este tipo de ataque se caracteriza por lo siguiente:

- Se puede adentrar fácilmente.
- ¡Desean siempre brindar ayuda!
- Es nuevo en la empresa.

[38] MARINO DODGE, Juan. Ataque - Ataque – Smishing. En: Conferencia Fraude Electrónico [Figura]. Memorias. Bogotá D.C., 2017. p. 24-28 http://acis.org.co/archivos/Conferencias/2017/Conferencia0211.pdf

- ¡No sé nada!
- Enlace remoto.
- Número telefónico reconocido.
- Representa a 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.

9.1.6 Ataque en persona

En este tipo de ataque una persona se hace pasar por empleado y solicita información para el acceso al sistema.

Ejemplo:

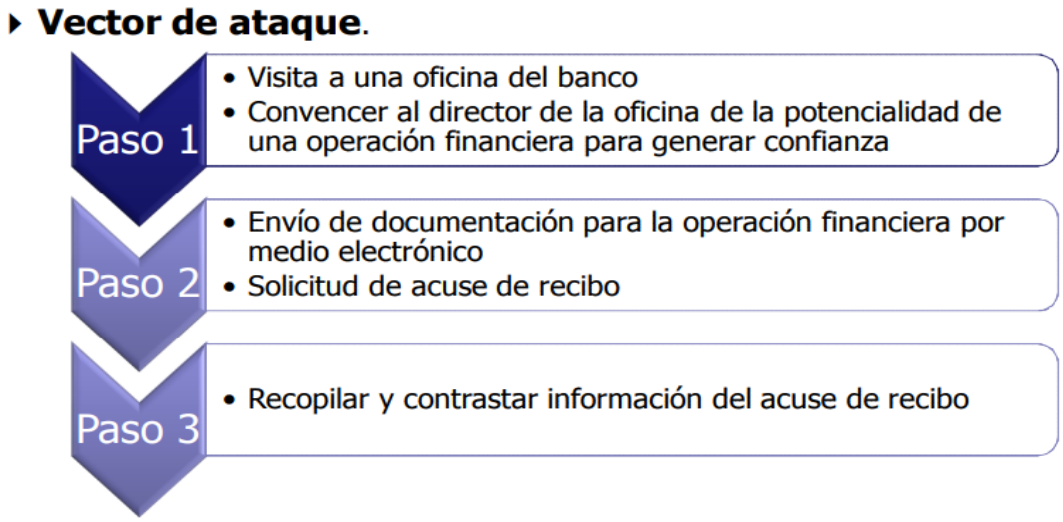
Atacante: Buenos días, mi nombre es Andrés soy el nuevo ingeniero civil y requiero el código para el ingreso al sistema....

Víctima: Mucho gusto ingeniero el código para el acceso es...

a) Caso presentado:

Asaltando un banco

Figura 7. Secuencia de pasos de un Vector ataque ingeniería social[39]



"Ejecución del vector.

- Se consiguió la versión y el nombre exacto del administrador de correo electrónico.
- Tanto los datos de enrutadores, gestión de tráfico y DMZ fueron obtenidos.
- Posteriormente se desarrolló un ataque al administrador de correo electrónico de modo exitoso.[40]

9.1.7 Quid Pro Quo

Los atacantes prometen un beneficio a las víctimas, pero estas tienen que otorgar información a cambio como usuarios y contraseñas un ejemplo muy claro es: Identificar una falla en el sistema y llamar para ofrecer soporte técnico y solventar el problema, pero pide credenciales de login de mentado sistema.[41]

---

[39] MONTERO, D., OWASP Andalucía Chapter Leader & Grupo iSoluciones (2007) Asaltando un banco, Vector de ataque. [Figura]. Recuperado de: https://docplayer.es/15753809-Owand-11-granada-ingenieria-social.html

[40] MONTERO David, Ingeniería Social, OWASP, 2007, [En línea] disponible en https://docplayer.es/15753809-Owand-11-granada-ingenieria-social.html

[41] LOPEZ Carlos, Ingeniería Social: El Ataque Silencioso, Revista Tecnológica No 8 2015, disponible en http://www.redicces.org.sv/jspui/bitstream/10972/2910/1/Articulo6.pdf

9.1.8 Dumpster Diving

En esta técnica el atacante le ofrece a la víctima beneficio a cambio de información delicada del mismo usuario o la organización. Por ejemplo, un ciber-delincuente puede investigar a un empleado y le ofrece un incentivo, pero debe dar datos críticos.[42]

9.1.9 Las cartas nigerianas

Conocidos así los mensajes falsos que nos llegan invitándonos a conseguir una gran cantidad de dinero a cambio de un desembolso inicial. Un caso frecuente es el de la herencia millonaria que ha tenido la gentileza de compartir con nosotros. Otra modalidad es el premio de lotería con el que hemos sido agraciados sin ni siquiera haber jugado.[43]

9.1.10 Shoulder surfing

Espionaje de los usuarios para la obtención de nombres de usuario y contraseña, mediante la observación directa de lo que teclea en el ordenador técnica de mirar por encima del hombro.

9.1.11 Vishing

Surge de la unión entre voice + phishing o más conocido como suplantar voz o telefonía, este se basa 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.

Vishing capitaliza la confianza de una persona en el servicio telefónico, ya que la víctima generalmente no tiene conocimiento de la capacidad del estafador de utilizar técnicas como la identificación de llamadas spoofing y sistemas automatizados avanzados para cometer este tipo de estafa.[44]

---

[42] PISCITELLI Emiliano. Ingeniería Social: Cuáles son los tipos de ataque, RedUSERS. 2015, Disponible en http://www.redusers.com/noticias/ingenieria-social-cuales-son-los-tipos-de-ataque/

[43] CSI CONSULTORES, Ingeniería Social, las técnicas con las que engañan a tu mente, 2016, Disponible en: https://www.maestrodelacomputacion.net/ingenieria-social-tecnicas-enganan-mente/

[44] YEBOAH, Ezer. MATEKO, Priscilla. Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices, Journal of Emerging Trends in Computing and Information Sciences.

9.1.12 Pharming

Conocido como la alteración de la "Resolución de Nombres de Dominio" donde un código malicioso, se introduce en el ordenador mientras realizamos ya sea descargas, copia de archivos de algún medio, correo electrónico u otro. La resolución de nombre de dominio es producida en el momento que se ingresa la dirección de un sitio web por ejemplo www.jaimesedanop.com esta URL es traducida a dirección IP (Internet Protocol) ej. 200.21.200.16 este procedimiento lo realiza los famosos DNS (Servidor de Nombre de Dominio).

El desarrollo de un pharming consiste en que, estando nuestro ordenador infectado por un código malicioso o software que posibilite la realización de cambios a DNS, al momento de intentar acceder a una página web introducimos la URL y confiando de que es el sitio web deseado, procedemos a realizar compras o cualquier otra transacción electrónica llevando a que el atacante obtenga claves de seguridad y por consiguiente la puerta abierta para adelantar fraude.[45]

Como evitar el Pharming:

Evite abrir e-mails no solicitados o que sean de una procedencia dudosa. 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.

Haga uso de 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 las debidas 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

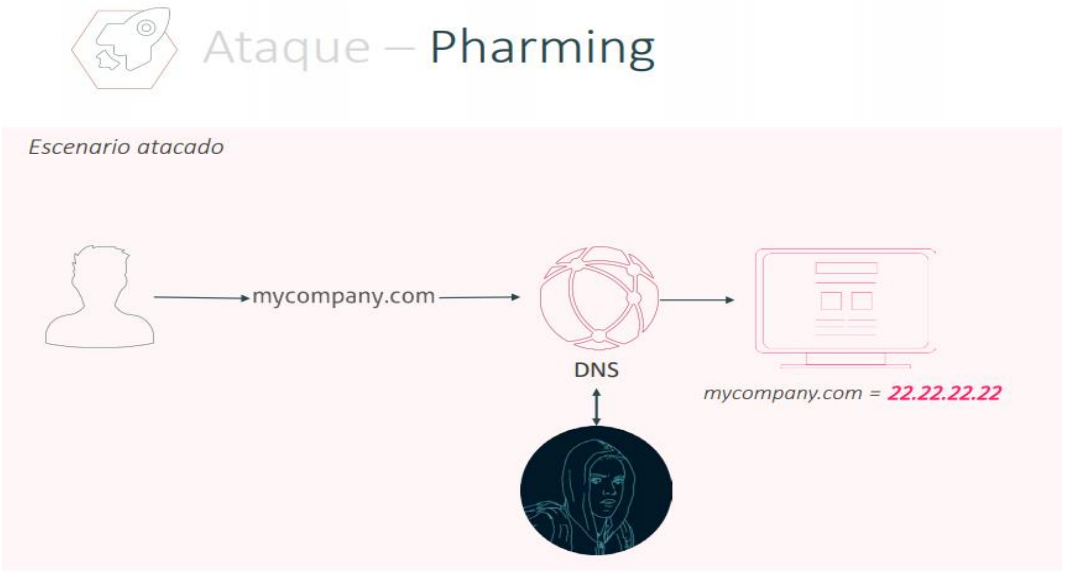
---

2014, Disponible en: https://pdfs.semanticscholar.org/7a27/1a3ff90b2a19d6b4f4ecc800e0aebdcda063.pdf

[45] CALLEGARI, Osvaldo. Delitos informáticos: Pharming. En: Negocios de Seguridad. Vol.; 1. No 031 (May.2007); p. 176. http://www.rnds.com.ar/revistas/031/RNDS_031.pdf

mundial.[46] El procedimiento de un ataque pharming lo podemos visualizar en la Figura 8.

Figura 8. Ataque - Pharming[47]



9.1.13 Malware Android.FakeTrojan.A

El malware suele venir en aplicación que, cuando se ejecuta, se muestra al usuario haciendo creer que es un software confiable para la generación de identificador único de acceso a la banca en línea. La aplicación se personaliza para múltiples bancos con logotipos y colores reales, un ejemplo claro es el evidenciado en la Figura 9.[48]

[46] Ibíd., p.180

[47] MARINO DODGE, Juan. Ataque - Ataque – Pharming. En: Conferencia Fraude Electrónico [Figura]. Memorias. Bogotá D.C., 2017. p. 35 http://acis.org.co/archivos/Conferencias/2017/Conferencia0211.pdf

[48] RANCHAL Juan, Robo de datos bancarios en Android por ataques de ingeniería social, 2012, disponible en https://www.muyseguridad.net/2012/03/16/robo-datos-bancarios-android-ataques-ingenieria-social/

Figura 9. Ejemplo Malware Android Fake Trojan[49]

9.1.14 CryptoLocker

Por medio del cryptolocker se busca que sea la misma persona quien lo ejecute basado en técnicas de ingeniería social. Precisamente el usuario accede a un correo que recibe y aparenta ser de una organización confiable, y este lleva un fichero adjunto tipo ZIP con una contraseña. Esta es una nueva clase reciente de ransom cuyo patrón de negocio se fundamenta en la extorsión al usuario.[50]

La instalación del troyano se realiza gracias a la ejecución de este adelantado por el usuario (victima) quedando como residente en el equipo:

- El troyano se instala en la carpeta donde está ubicado el perfil del usuario la cual puede ser AppData o LocalAppData.

- Se crea una ejecución al reinicio por medio de un autorun y se asegura.

[49] RANCHAL J. Robo de datos bancarios en Android por ataques de ingeniería social, (2012), [Figura]. Recuperado de: https://www.muyseguridad.net/2012/03/16/robo-datos-bancarios-android-ataques-ingenieria-social/

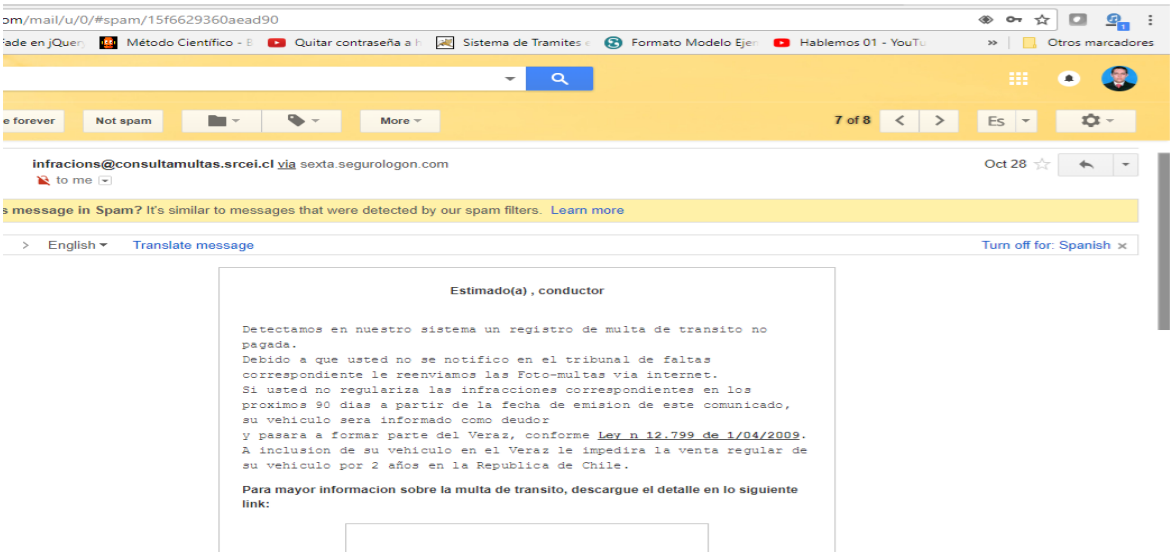
[50] PANDA SECURITY, CryptoLocker: Qué es y cómo evitarlo, 2015, disponible en https://www.pandasecurity.com/spain/mediacenter/malware/cryptolocker/

- Ejecuta dos procesos. El principal y un segundo para blindar el proceso original ante posible cierre.[51]

9.1.15 Spam

Entendido como correos electrónicos no deseados, los cuales pueden llevar publicidad, virus u otro fin, por lo general suelen ser remitentes desconocidos o no incluidos en libreta de direcciones;[52] es por medio de estos que los atacantes pretenden engañar al usuario informando que recibimos un correo legítimo y puede venir inmerso un virus o link para acceder a otra página como nos lo deja ver la multinacional ESET en su artículo (El spam y la Ingeniería Social, 2008) y un ejemplo claro de esto se puede ver en la siguiente imagen.

Figura 10. Ejemplo de recepción de correo Spam con link de multa (Autor)



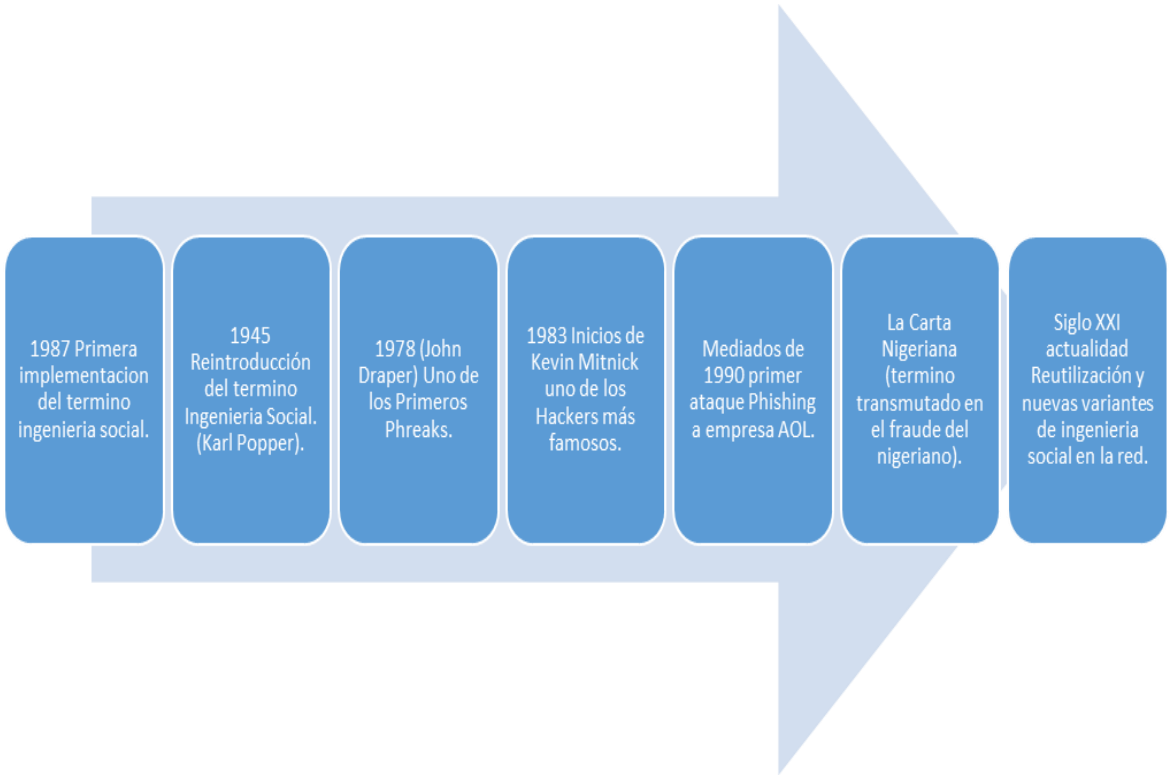
[51] Ibid.

[52] ZOTTO Rodolfo S. "Spam" o correo electrónico no deseado, Editorial ASTREA, pp2, 2004, Disponible en: https://www.astrea.com.ar/resources/doctrina/doctrina0140.pdf

10. ANALISIS HISTÓRICO ATAQUES DE INGENIERÍA SOCIAL EN EL MUNDO

Durante el transcurrir de la historia, la ingeniería social ha ido tomando diferentes connotaciones influyendo de una u otra forma los avances tecnológicos, por lo que a continuación se muestra un breve recorrido de los hechos significativos en la historia y se pueden detallar en la Figura 11.

Figura 11, Breve historia de la ingeniería social[53]



Con el transcurrir del tiempo a nivel mundial se han presentado múltiples casos de ingeniería social, donde estos son llevados a cabo por los cibercriminales poniendo en riesgo información y el dinero de usuarios o empresas. A continuación, se describen una serie de ataques ocurridos a lo largo de la historia, estos son solo algunos de los muchos que puedes surgir:

[53] SEDANO PINZON, Jaime. Breve historia de la ingeniería social [Gráfico], 2019

10.1 INGENIEROS SOCIALES EN ESPAÑA y EEUU[54]

Agnus Young

Agnus un joven de tan solo 14 años de edad, era una persona que sabía mucho de Phreaking en España a inicios de la década de los 90. Con un teclado que mantenía cubierto por típex blanco y entintado con color fluorescente de rotulador, escuchando música de la Polla Record 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 antiguo. Todas las noches llevaba a cabo conexión a líneas internacionales de múltiples carriers y escribía documentos donde los demás hackers implementaban para llamar gratis a cualquier lugar.

D-Orb

Una señora que se encuentra en una tienda de modas se acerca a la caja con múltiples prendas acompañada de su hija la cual tenía 14 años de edad, la cajera realiza la suma total de la adquisición y procede a entregar la tirilla y la cliente saca su tarjeta MASTERCARD para el pago.

La cajera coge la tarjeta y la pasa por la maquina lectora e imprime los datos de nombre y número en el formulario pequeño con múltiples copias carbonadas. Seguidamente procede a llamar a la central de autorizaciones de la empresa la cual pertenecía la tarjeta y consulta. La llamada dura unos minutos y al final la cajera le entrega a la clienta el formulario y un lapicero para firmar la compra.

D-Orb ubicado cerca de un aparador, como si estuviera visualizando prendas para dama de la tienda, detalla toda la operación llevada a cabo, cuando la mujer sale de la tienda este se dirige hacia un establecimiento que hay junto en frente y llama al número que lee por fuera de las bolsas que lleva la cliente al salir de la tienda.

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

- Si, ¿en qué le puedo servir?

[54] LESTER THE TEACHER, INGENIERIA SOCIAL 1.0 Hasta Cap IV-VII, 2002, España, Disponible en: http://www.netcomunity.com/lestertheteacher/doc/ingsocial1.pdf

- 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 vera 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 en ningún momento presentó alguna duda de lo que estaba brindando al hacker, donde los datos brindados podrían ser utilizados en cualquier lugar del mundo desde ese momento y algo mucho más importante el número de identificación de la tienda en MASTERCARD.

Con todos los datos proporcionados podría llamar a MASTERCARD y verificar el saldo de cualquier tarjeta generada con multiplicidad de aplicaciones que producen números validos de MASTERCARD. D-Orb con solo 15 años de edad ya manejaba múltiples idiomas.

Omega

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 realizaba por medio de un software "wardialing" (Encargado de realizar llamadas automáticas a números de teléfono y guardaba los resultados en bases de datos).

En aquellos momentos las centrales no contaban con la función de "caller ID" y las líneas eran análogas siendo poco sencillo tracear llamadas.

Hacker Ciego al FBI año 2005

En EEUU, en la central de emergencias suena la línea 911 y al otro lado de esta 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 la sencilla razón y es porque su papá violó a mi hermana dejándola inconsciente.[55]

El atacante se identifica como John Defanne. Desde la central de emergencias realizan una verificación del número. Se trataba de la casa de los papás de Danielle, que tenía para la época 19 años, en un suburbio de Colorado Spring. Desde el otro lado de la línea Defanne continúa hablando: Golpee al padre con mi arma y está desangrando profundamente. Estoy armado, tengo un revolver. Les dispararé sin dudarlo en caso de encontrar policías cerca, será mejor que consigan ayuda por parte de ustedes porque me estoy volviendo por momentos loco.

El operador que atendía la llamada en la oficina de emergencias intenta mantener a Defanne en la línea, pero este la termina abruptamente con un mensaje: voy a colgar, ya tienen la dirección, si no llega nadie para ayudarme en los próximos seis minutos juro por Dios, ¡los voy a joder!, y les voy a volar los sesos a los dos.

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.[56]

[55] JORGE, Miguel, Pioneros de la ingeniería social: el hacker ciego que puso de rodillas al FBI, PHREAKS, 2016, Disponible en: https://es.gizmodo.com/pioneros-de-la-ingenieria-social-el-hacker-ciego-que-p-1789268307

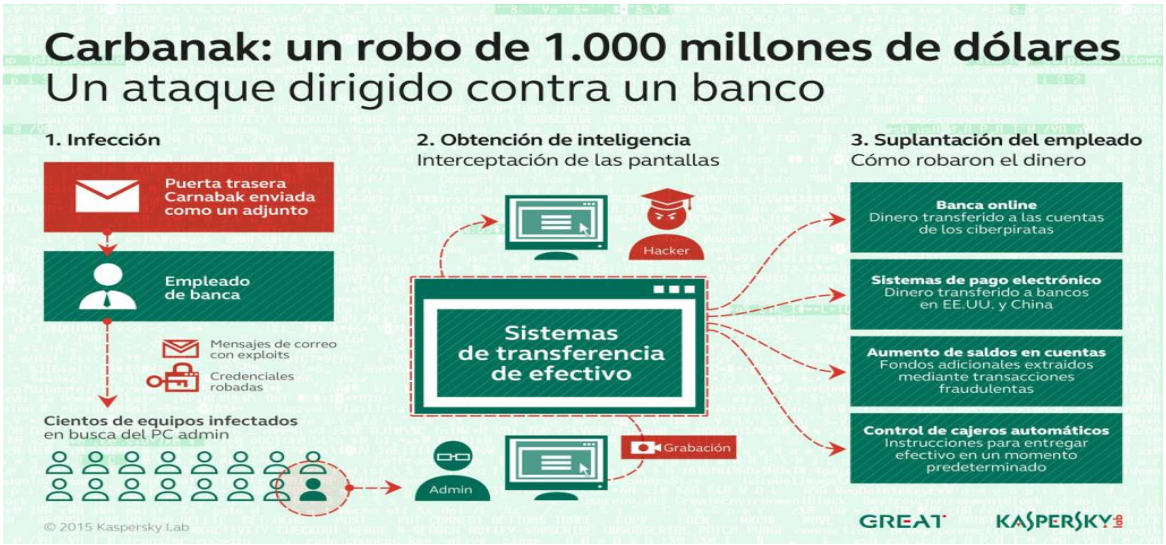
[56] JORGE cit.

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.[57] El desarrollo del ataque puede visualizarse en la figura 12.

Figura 12. Carbanak un robo de 1000 millones de dólares[58]



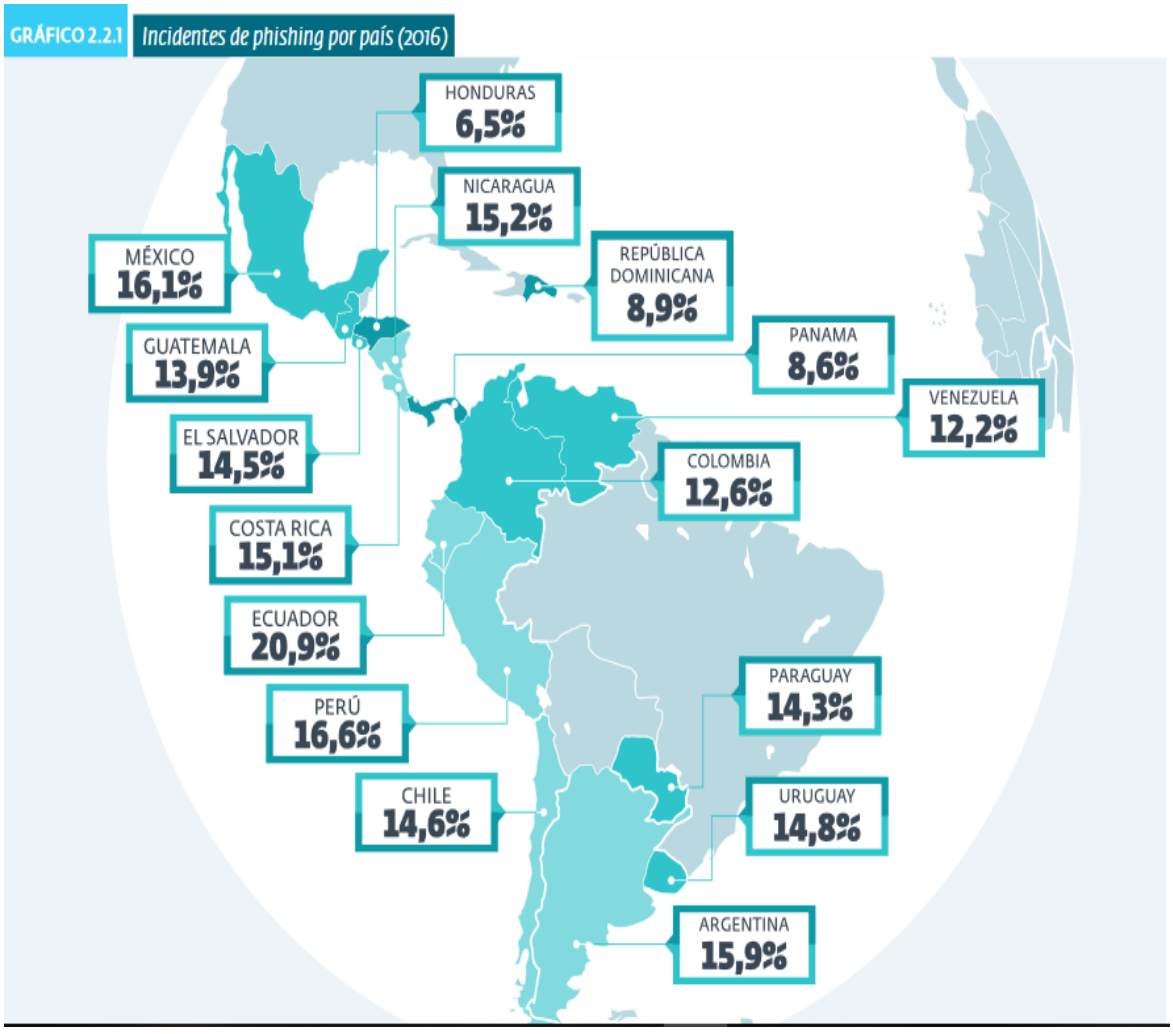
[57] EMM David, NIKISHIN A. & GOSTEV A. Kaspersky Security Bulletin 2015. Principales incidentes de seguridad, KASPERSKY, 2015, Disponible en: https://securelist.lat/kaspersky-security-bulletin-20152016-die-top-security-stories/82250/

[58] EMM David, NIKISHIN A. & GOSTEV A. Carbanak, Kaspersky Security Bulletin 2015. Principales incidentes de seguridad, KASPERSKY, [Grafico] 2015, Disponible en: https://securelist.lat/kaspersky-security-bulletin-20152016-die-top-security-stories/82250/

10.2 INCIDENTES EN COLOMBIA Y LATINOAMERICA

Teniendo en cuenta los vertiginoso que ha avanzado la tecnología a nivel nacional e internacional y su incidencia en las labores diarias, la multinacional ESET Security para el año 2017 nos presenta el reporte de incidentes asociados al Phishing en Latinoamérica, donde se evidencia un 12,6 % presentado en Colombia durante el año 2016 y es mostrado en la figura 13.

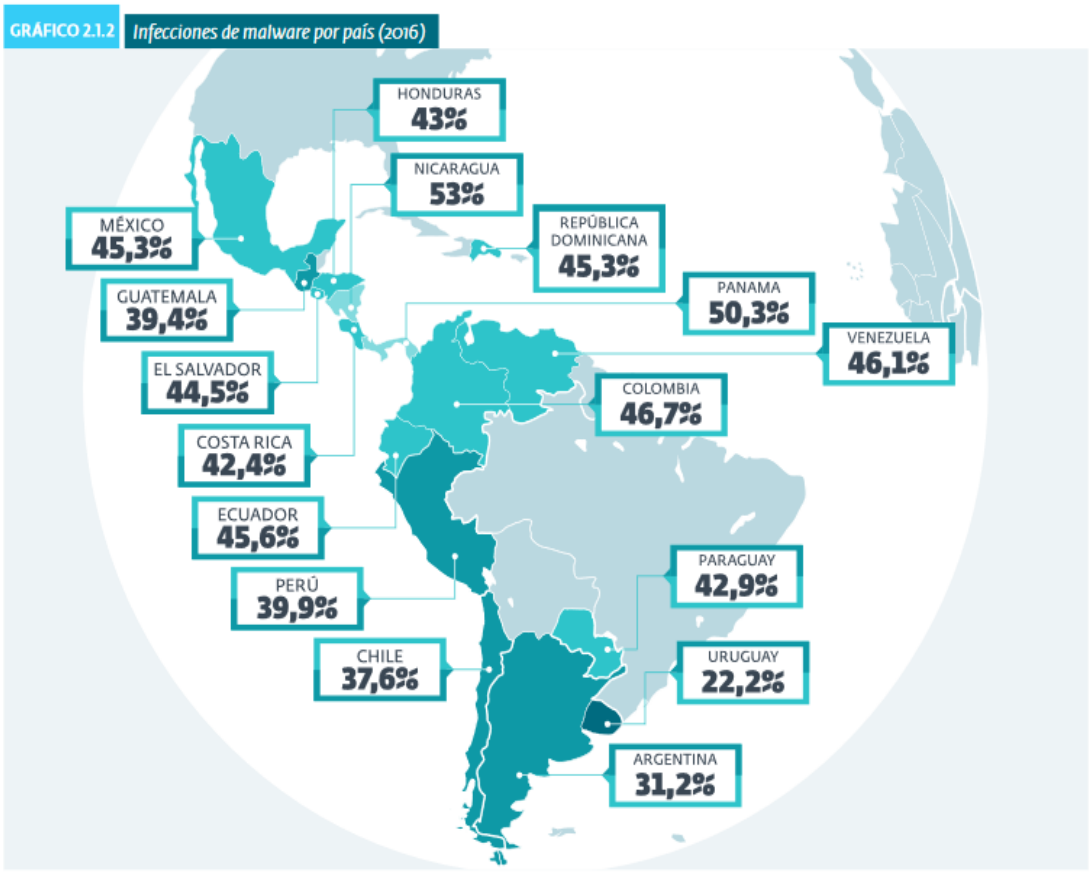
Figura 13. Incidentes de Phishing por país (2016)[59]



[59] ESET Security Report Latinoamérica, Incidentes de phishing por país 2016, (2017), Disponible en https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

Con la ingeniería social se puede llegar a ser víctima de infecciones provocadas por malware; a nivel de Colombia se han presentado un porcentaje alto lo cual se evidencia en el reporte elaborado por ESET Security del año 2017, pudiéndose visualizar en la Figura 14.

Figura 14. infecciones de malware por país (2016)[60]



[60] ESET Security Report Latinoamérica (2017) Infecciones de malware por país 2016. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

10.3 Casos De Vida Real a Empresas y Usuarios

10.3.1 Ingeniería social de modo inverso 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 llevaran a cabo este tipo de estafas.[61]

10.3.2 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.

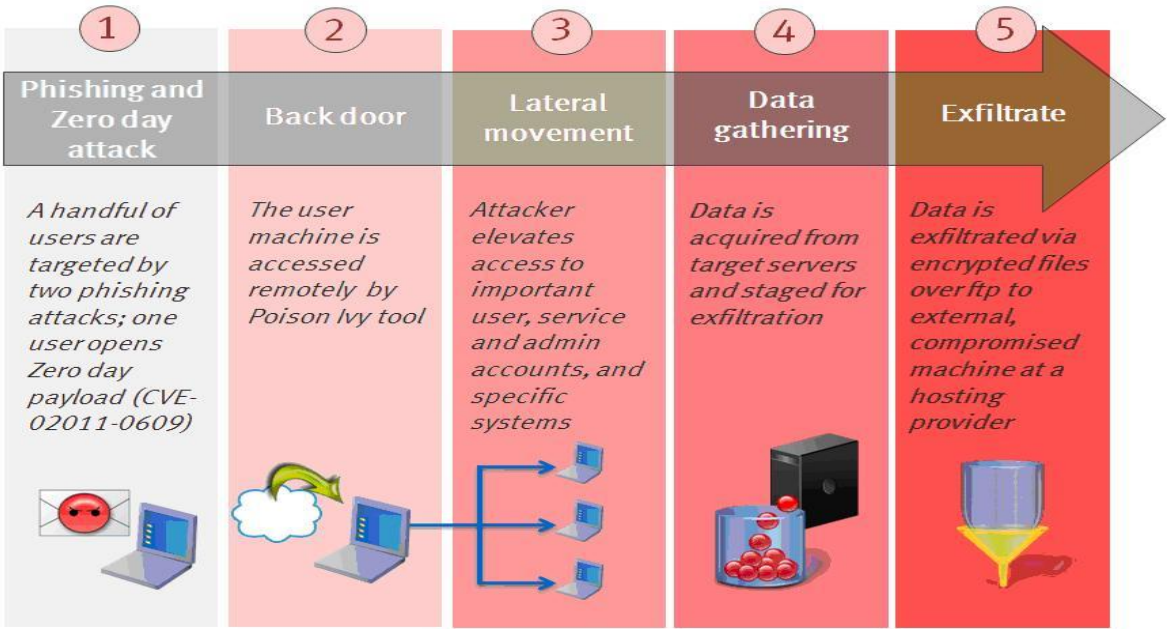
La apertura de ficheros ofimáticos que vienen adjuntos en e-mails son una constante de muchos usuarios que tienen las defensas bajas ante archivos PDF, Excel y ODF. Cuando es explotada la vulnerabilidad se instala una versión modificada de Poisson Ivy, una de las RAT más famosas, la cual permite: encender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

Desde la consola de Poisson Ivy, el atacante procedió a recoger información, crackear cuentas de usuarios y servicios para conseguir privilegios que le permitieran acceder a repositorios de datos en servidores internos. Con la versión morpheada de Poisson Ivy el atacante logró saltar antimalware de endpoint. Dejando entredicho la confianza en las herramientas y la necesidad de confiar más en unas políticas estrictas. Tras obtener los datos que deseaba, se cifraron y

[61] SANTIAGO Sarah, Ingeniería social, cuando blindar sistemas informáticos no lo es todo [En linea] Seguridad Informática para Todos, 2017, disponible en https://opendatasecurity.io/es/ingenieria-social-cuando-blindar-sistemas-informaticos-no-lo-es-todo/

enviaron por FTP a un servidor para quedarse con la información; en la Figura 15 se puede evidenciar como se adelantó el ataque.

Figura 15. Secuencia pasos de un ataque a RSA[62]



10.3.3 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, el Upatre descarga y ejecuta el troyano Dyre en el equipo de la víctima. La mayoría de los programas antivirus no lo detectaron.

Este troyano tiene capacidad de retener la libreta de direcciones de la víctima y enviar e-mails masivos a todos ellos a través de Outlook. El malware vigila las actividades de la víctima y se queda a la espera, cuando la víctima intenta iniciar sesión, Dyre muestra una nueva pantalla con un mensaje indicando que el sitio está experimentando fallas y que se debe llamar al número proporcionado para adelantar la transacción.

[62] CHEMA Alonso, La RSA explica el ataque que sufrió, 2011, disponible en: http://www.elladodelmal.com/2011/04/la-rsa-explica-el-ataque-que-sufrio.html

Al llamar al número el usuario es atendido por una persona real. Los atacantes luego de obtener la información de la víctima tan pronto como se cuelga el teléfono, proceden a realizar transferencias bancarias. Y para eludir la detección por el banco la página web de la organización objetivo sufre un ataque DDoS con la finalidad de evitar que la víctima pueda acceder a la cuenta del banco.[63]

10.3.4 Medios Noticiosos utilizados en Ingeniería Social

Los desastres naturales o los eventos de lanzamiento son muy implementados a la hora de realizar ataques de ingeniería social, donde la victima principal es el usuario mismo, todo debido a que es en muchas ocasiones difícil resistirse y no nos tomamos el tiempo de verificar si es real o falso. Los ciber-delincuentes se afanan en poner trampas, creando sitios maliciosos en muchos de los casos para que el usuario ejecute malware generando desastres en su sistema.

- Desastre Natural:

  Después de que ocurriera el tsunami de Japón en el año 2011, determinadas páginas web de noticias falsas infectaron los sistemas de los usuarios que pretendían mantenerse informados, todo fue a través de un malware FAKEAV que se alojaba en los sitios web.

- Lanzamiento de Producto o Servicios:

  Por medio de un correo electrónico se logró engañar a múltiples usuarios a través de una falsa promoción en la que se solicitaba información personal para regalar un iPad.

Las noticias sobre personalidades es otro de los puntos muy implementados para el engaño, todo está en cautivar al lector para ganar fans lo que el atacante aprovecha para colgar link de videos y fotos de determinado personaje.

- Escandalo:

  En una red social se promocionaba un video donde "acababa con la carrera de Justin Bieber para siempre" pero en realidad se direccionaba a los usuarios a una página web de encuestas y finalizaba en sus propias páginas.

- Controversia

[63] THE HACKER NEWS, Dyre Wolf roba más de 1 millón de dólares por transacción, 2015, Disponible en: https://www.seguridad.unam.mx/historico/noticia/index.html-noti=2216

Por medio de una imagen difundida por MSN se invitaba a usuarios para que descargaran un fichero jpg relacionado con la muerte de Michael Jackson, pero en realidad se almacenaba un malware en el computador de las víctimas.

- Muerte Falsa

  Con el rumor que se había muerto Jackie Chan, un sitio web de noticias falsas redirigía a las víctimas a una página web maliciosa.[64]

[64] TREND MICRO, 5 Motivos por los que las trampas de la ingeniería social funcionan, 2012, Disponible en: http://www.trendmicro.es/media/br/5-reasons-why-social-engineering-tricks-work-es.pdf

11. MEDIDAS PREVENTIVAS ANTE LA INGENIERÍA SOCIAL

a. Uso de aplicaciones corporativas de modo seguro: Es importante que el acceso y uso de aplicaciones corporativas se realice siguiendo políticas de seguridad, donde en caso de requerir internet se haga bajo una conexión segura, de igual forma solo el personal autorizado tiene que estar facultado para su implementación, gestión de copias de seguridad periódicas e ingreso de datos a procesar.

b. Utilización de servicios web de modo seguro: Antes de acceder a páginas web para transacciones u otro tipo de manejo de información, se tiene que utilizar conexiones seguras, digitando manualmente la URL y evitar utilizar buscadores ya que no todos los resultados mostrados son correctos y se puede caer en una suplantación y robo de información.

c. Evitar descargar archivos de correos electrónicos no conocidos: Vía emails se pueden llegar a recibir mensajes solicitando descargar archivos y acceso de otro contenido, lo cual pone en riesgo la seguridad del sistema e información, se tendrá que evitar guardar archivos de correos no conocidos y procurar utilizar también antivirus que analicen contenido de la red.

d. Conocimiento de las técnicas más frecuentas de ingeniería social: Es fundamental conocer cómo funcionan cada una de las técnicas tanto actuales como antiguas, donde se tenga un plan de formación y de mitigación de riesgos asumiendo una cultura preventiva para evitar ser víctimas; con cada dispositivo tecnológico nuevo que se utilice se tendrá que evaluar posibles ataques que se puedan gestar.

e. Tener presente la legislación sobre el manejo de la información y delitos informáticos, tanto del territorio nacional como el internacional, para el caso de Colombia la Ley 1273 de 2009 promulgada por el congreso de la republica nos brinda un instrumento para cuidar la información que se maneja, de igual forma a nivel mundial se tiene el Convenio sobre la ciberdelincuencia, adoptado el 23 de noviembre de 2001, en BUDAPEST, este último es muy utilizado como referencia para otras legislaciones.

f. Mantener una actitud cautelosa: Antes de brindar cualquier ayuda o de recibirla, es fundamental tener precaución en no dar información reservada y no dejar que los productos sean manejados por personas no autorizadas, muchas solicitudes de ayuda son falsas y buscan una vulnerabilidad para acceder a sistemas o datos.

g. Verificar con quien se habla tanto vía telefónica como personal: para prevenir falsas identidades, es fundamental corroborar con quien se está tratando, si es de

una empresa se tiene que contactar y solicitar verificación de la identidad como Nro. De empleado, cargo entre otros, no todo el que se hace pasar por soporte o encargado de sistemas es realmente la persona que dice ser, sea precavido y no ponga en riesgo su seguridad.

h. Evite que lo intimiden o adulen para dar información: no se deje intimidar por cualquier persona y en caso tal de dudas recurra a la ayuda de profesionales certificados para recibir una correcta orientación antes de tomar cualquier decisión, tenga cuidado con publicar información confidencial que haga que lo amenacen.

i. No se deje sorprender por conocimientos exhibidos, muchos ciber-delincuentes muestran supuesta sabiduría para que termines dando información y luego terminar siendo víctima de un fraude; mucho puede sonar como parte de la cosa más real del mundo, pero puede terminar siendo una conspiración, tenga cuidado con lo que le están mostrando o haciendo ver.

j. Tenga cautela con lo que le ofrecen tanto encuestas, concursos, ofertas u otro producto por cualquier medio de comunicación, no todo lo ofrecido es real y pueden llevarlo a que brinde información de tarjetas de crédito o información confidencial, antes de tomar un producto o servicio, contacte a la empresa y corrobore la veracidad de esto, así como términos y condiciones para no tener que lamentar.

k. No responda a solicitudes por MSN, llamada o correo electrónico, las entidades nunca solicitan datos de tarjetas de crédito, usuarios, contraseñas o cualquier otra información personal a través de estos medios ellos ya la tienen, en caso de olvido diríjase a la organización respectiva y pida ayuda para recuperar credenciales o bloqueo de algún producto contratado.

l. Evite el uso de redes punto-a-punto o P2P: Los archivos compartidos en estas pueden transportar virus ya que la mayoría de ellas son desprotegidas, algunas de estas redes pueden ser eMule, Ares, Kazaa, Imesh u otra, si requiere transmitir alguna información o descargar algo, recurra a redes seguras donde se implementen protocolos y encriptación. También haga uso de sistemas de autenticación como firma digital, biometría, etc.

m. Evite tomar decisiones bajo presión, si alguien le pide que tome una elección de carácter urgente, sea precavido y use todo el tiempo que este a su disposición para no correr riesgos, de igual forma puedes recurrir a las autoridades en caso de sospechar de algo irregular ante posibles fraudes, a su vez tenga precaución con las palabras o discursos que escucha por teléfono ya que pueden hacer que opte por una decisión sin darse cuenta.

m. No se deje envolver con cosas que son demasiado buenas para ser verdad, un ejemplo puede verse en lo relacionado a premios ganados, pero a cambio le

solicitan consignaciones o datos de cuentas bancarias, que en realidad buscan es robar fondos o información de sus productos financieros, procure hacer caso omiso y denunciar ante las autoridades pertinentes.

11.1 FORMACIÓN DE USUARIOS

Una de las principales y efectivas medidas de seguridad es sin duda la adecuada preparación técnica de los administradores de la red y del sistema informático, teniendo en cuenta los usuarios y directivos. Dentro de las políticas están las leyes que cobijan el uso y manejo de la información.

Los temas que se deben aplicar en cualquier formación de los usuarios están:

a) Utilización segura de las aplicaciones tanto corporativas como particulares.

b) Utilización segura de los servicios que hayan sido autorizados entre los que pueden estar: Navegación en Internet, implementación de firmas electrónicas, criptografía y garantizar la Integridad, confidencialidad y disponibilidad de la información.

c) Reconocer la información que se recibe en los e-mails.

d) Reconocer las técnicas más frecuentes de Ingeniería Social.

e) Conocer las obligaciones y responsabilidades que se asumen por el uso de la información.

f) Saber gestionar soportes informáticos. Todo lo anterior puede cobijarse en un manual de uso, que el usuario debería tener.[65]

[65] GOMEZ, Álvaro. Enciclopedia de la Seguridad Informática, Ingeniería Social, 2ª Edición, México DF, ALFAOMEGA GRUPO EDITOR S.A, 2014, 134p.

12. METODOLOGÍA DE DESARROLLO

Fase Inicial:

Identificación de la problemática a estudiar donde fue necesario recurrir a fuentes bibliográficas tanto físicas como digitales para la indagación, consulta, recopilación y organización adecuada de la información a utilizarse.

Fase 2:

Se Recolectaron las fuentes bibliográficas teniendo en cuenta las que son primarias y secundarias, desglosando el tema de ingeniería social desde sus orígenes hasta el nuevo siglo, luego se procede a un análisis de clasificación de las diferentes técnicas desde el antes y el ahora.

Fase 3:

Una vez que se ha clasificado y revisado la información, se comenzó a elaborar el documento partiendo por la formulación del problema con sus antecedentes y la estructura requerida, teniendo en cuenta las técnicas surgidas en el tiempo desde 1950 origen hasta el año 2017.

Fase 4:

Después de analizadas cada una de las técnicas junto con las medidas preventivas, se procede a generar las recomendaciones a tener en cuenta tanto de cómo prevenir los ataques de ingeniería social hasta la manera de cómo educar al usuario para que sea más responsable con la información que maneja.

CONCLUSIONES

Con el desarrollo de la presente monografía se ha logrado visibilizar diferentes técnicas de ingeniería social que se han venido gestando con el transcurrir de la historia, todo basado en una indagación en múltiples fuentes bibliográficas donde se empieza conociendo la temática y terminología relacionada, para luego pasar a analizar los pasos de cómo se llevan a cabo los ataques; esto ha permitido evidenciar lo frágil que es el ser humano a factores como la influencia y el desconocimiento. Muchas de las técnicas actuales han sido mejoradas o son el retoño de las primeras surgidas en años anteriores.

Por medio de la indagación se han encontrado muchos casos de la vida real que han derivado en múltiples pérdidas millonarias tanto para empresas como para usuarios, viéndose afectada la confianza y la seguridad en el manejo de tecnología. También se logra conocer que técnica se utilizó en dicho caso y quien resultó más vulnerable a estos ataques, de igual forma los estudios desarrollados por multinacionales dejan ver los porcentajes presentados en algunos países de Latinoamérica.

La revisión y el análisis de lo relacionado a ingeniería social lleva a tomar un tema que, aunque no se profundizó se tiene en cuenta para interpretar como un ciber-delincuente lleva a cabo un ataque, y es la persuasión e influencia las herramientas que no puede faltar a la hora de engañar a un usuario para que realice algo pensando que es correcto. También se describen las finalidades y motivaciones que llevan a los ingenieros sociales a atacar.

La educación de los usuarios se ha dejado muy de lado, pensando que tener un software sofisticado es la solución perfecta a la hora de evitar un ciberataque; teniendo en cuenta que la tecnología avanza y los ciber-delincuentes no se quedan quietos, la formación tendrá que ser permanente sin olvidar los ataques ocurridos anteriormente, ya que muchas técnicas actuales son un derivado de lo que ya ocurrió y de nuevas estrategias para lograr hacer caer a la víctima.

Con la revisión de las diferentes técnicas se logra establecer que no es muy acertado indicar que una sea la mejor de todas, ya que cada una puede desarrollarse en un contexto determinado y aunque se presenten muchos ataques vía correo electrónico, también se pueden realizar con el teléfono, por medio de instalación de software especializado o el descuido mismo de la persona al dejar visible información reservada; por lo que el concientizar al usuario del valor que tienen los datos, como manejarlos desde que se elabora hasta su almacenamiento puede mitigar futuras perdidas y riesgos innecesarios.

RECOMENDACIONES

Mantener en formación permanente sobre temas de seguridad informática, especialmente los últimos ataques de ingeniería social que permita promover un ambiente de protección de la información en cualquier ámbito en el que se encuentre el usuario. Estas capacitaciones se tienen que llevar a cabo de modo periódico teniendo en cuenta tanto lo que ya paso y lo que pueda venir.

Para las empresas se recomienda elaborar un manual de políticas de seguridad, donde se den a conocer lineamientos sobre cómo manejar la información desde el momento en el que se genera hasta cuando se transportada en los diferentes medios, evitando daños en su integridad, confidencialidad y disponibilidad a su vez se tendrá que controlar el acceso a los diferentes dispositivos tecnológicos.

Asumir medidas preventivas ante posibles ataques de ingeniería social como copias periódicas en servidores alternos o haciendo uso de servicios en la nube teniendo suma precaución en poder acceder a páginas de internet seguras e ir más allá del certificado de seguridad, ya que este no garantiza en su totalidad que un sitio web sea seguro.

Mantener revisando con suma precaución los contenidos recibidos vía correo electrónico y por otros medios como USB, CDs, a su vez evitar compartir credenciales de acceso personal; ninguna entidad bancaria solicita actualización de información confidencial por ningún medio, para la recuperación de autenticación acercarse a la entidad respectiva.

Si bien durante la historia se han desarrollado diferentes ataques de ingeniería social con la finalidad de conseguir información o llevar a cabo ataques cibernéticos, todo en su mayoría ha sido por la persuasión y la influencia que logra conseguir el ataque, por lo que se recomienda no dejarse intimidar y ante la toma de decisiones asumir una actitud pensativa y razonable para elegir lo correcto y seguro.

BIBLIOGRAFÍA

ARCOS, Sergio. Ingeniería Social: Psicología aplicada a la seguridad informática. Trabajo de grado Ingeniería en Informática. [En línea] Barcelona, España: Universitat Politécnica de Catalunya. Departamento de Ingeniería de Servicios y Sistemas de Información, 2011. 22p. Disponible en: https://upcommons.upc.edu/handle/2099.1/12289

BARRERA IBÁÑEZ Silvia, La Ingeniería Social y Cibercrimen, [En línea], 2015, {15 octubre de 2017}, disponible en http://www.cajarural.com/rurales/blog/2015/ingenieria_social.pdf

BISCIONE Carlos A., Ingeniería Social para no creyentes, [En línea] Sun microsystems, disponible en http://52.1.175.72/portal/sites/all/themes/argo/assets/img/Pagina/IngenieraSocial_CarlosBiscione.pdf

BORGHELLO Cristian, El arma infalible: La ingeniería Social, [En Línea], Technical & Educational Manager de ESET Para Latinoamérica, 2009, disponible en http://www.eset-la.com/pdf/prensa/informe/arma_infalible_ingenieria_social.pdf

CALLEGARI, Osvaldo. Delitos informáticos: Pharming. En: Negocios de Seguridad. [en línea]. Vol.; 1. No 031 (May.2007); p. 176. http://www.rnds.com.ar/revistas/031/RNDS_031.pdf

CASTELLANOS Luis, Ingeniería Social, [En línea] 2009, disponible en https://goo.gl/MEAmTN

CASTILLERO M. Oscar, Persuasión: definición y elementos del arte de convencer, Psicología Social y Relaciones personales, [En línea], 2016, Disponible en: https://psicologiaymente.com/social/persuasion-definicion-elementos-convencer

CHEMA Alonso, La RSA explica el ataque que sufrió, [En línea], 2011, disponible en: http://www.elladodelmal.com/2011/04/la-rsa-explica-el-ataque-que-sufrio.html

COLOMBIA. CONGRESO DE LA REPUBLICA, Ley 1273 de 2009, Bogotá, Colombia, [En línea], Disponible en http://acueductopopayan.com.co/wp-content/uploads/2012/08/ley-1273-2009.pdf

COLOMBIA. CONGRESO DE LA REPUBLICA, Ley Estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, [En línea], 2013, Disponible en:

https://www.sisben.gov.co/Documents/Informaci%C3%B3n/Leyes/LEY%20TRATAMIENTO%20DE%20DATOS%20-%20LEY%201581%20DE%202012.pdf

COLOMBIA. CONGRESO DE LA REPUBLICA, Ley No 1928 de 2018, Por medio de la cual se aprueba el <<convenio sobre la ciberdelincuencia>>, adoptado el 23 de noviembre de 2001, en BUDAPEST, [En línea], Disponible en: http://es.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf

CSI CONSULTORES, Ingeniería Social, las técnicas con las que engañan a tu mente, [En Línea]. 2016, Disponible en: https://www.maestrodelacomputacion.net/ingenieria-social-tecnicas-enganan-mente/

DANHIEUX Pieter, Phishing por correo electrónico, [En Línea], Securing the human SANS, 2013, disponible en https://nanopdf.com/download/phishing-por-correo-electronico-securing-the-human_pdf

DINAMARCA. Royal Danish Defence College. Social Vulnerability & Assessment Framework - A Study on Social Engineering 2.0, Copenhagen, Dennis Hansen Editores, 2017, 67-69pp.

EMM David, NIKISHIN A. & GOSTEV A. Kaspersky Security Bulletin 2015. Principales incidentes de seguridad, KASPERSKY, 2015, Disponible en: https://securelist.lat/kaspersky-security-bulletin-20152016-die-top-security-stories/82250/

ESCUDERO C. JAVIER, Estrategias para persuadir, ISSN 1138-9702, Nº. 117, 2007, págs. 83-94, disponible en: http://www.infoservi.com/infoservi/descargas/45_Estrategias_Para_Persuadir.pdf

ESPAÑA. Escola Tècnica Superior d'Enginyeria Informàtica, Un Viaje a la Historia de la Informática, La Génesis del Ordenador Moderno, España, EDITORIAL UNIVERSITAT POLITÈCNICA DE VALÈNCIA, 2016, 15p, disponible en: http://museo.inf.upv.es/wp-content/uploads/2016/12/Un%20viaje%20a%20la%20historia%20de%20la%20informm%C3%A1tica.pdf

GOMEZ, Álvaro. Enciclopedia de la Seguridad Informática, Ingeniería Social, 2ª Edición, México DF, ALFAOMEGA GRUPO EDITOR S.A, 2014, 134p.

INTEL SECURITY. Ataques al sistema operativo humano, Intel Security, 2015, disponible en: http://www.ebankingnews.com/wp-content/uploads/2015/02/Informe-Ataques-al-sistema-operativo-humano_feb_2015.pdf

INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. Compendio, tesis y otros trabajos de investigación. Sexta Actualización. Bogotá. ICONTEC, 2008.

JORGE, Miguel, Pioneros de la ingeniería social: el hacker ciego que puso de rodillas al FBI, [En línea], PHREAKS, 2016, {15 octubre de 2017}, Disponible en: https://es.gizmodo.com/pioneros-de-la-ingenieria-social-el-hacker-ciego-que-p-1789268307

KARPERSKY LAB. ¡Que es el spear phishing?, 2017, Disponible en: https://latam.kaspersky.com/resource-center/definitions/spear-phishing

LEDESMA, Cristina; LEDESMA, Ana & PASCALE Maricarmen, Ingeniería social - El hackeo al ser humano. Un enfoque holístico, 2014, {16 octubre de 2017}, disponible en: http://www.magazcitum.com.mx/?p=2747

LESTER THE TEACHER, INGENIERIA SOCIAL 1.0 Hasta Cap IV-VII, [En línea], 2002, España, Disponible en: http://www.netcomunity.com/lestertheteacher/doc/ingsocial1.pdf

LUQUE José, Qué es el phishing y cómo protegerse, [En línea], ASOCIAT, 2005, Disponible en: http://seguridad.internautas.org/html/451.html

LOPEZ Carlos, Ingeniería Social: El Ataque Silencioso, Revista Tecnológica No 8 2015, [En línea], disponible en http://www.redicces.org.sv/jspui/bitstream/10972/2910/1/Articulo6.pdf

MARINO DODGE, Juan. Fraude Electrónico. En: Conferencia Fraude Electrónico, EASYSOLUTIONS, [en línea]. Memorias. Bogotá D.C., 2017. p. 23-28 http://acis.org.co/archivos/Conferencias/2017/Conferencia0211.pdf

MITNIK Kevin & SIMON William, El arte de la Intrusión, [En línea], EEUU: Alfa Omega Editor, ISBN 978-970-15-1260-9, 2007, disponible en https://radiosyculturalibre.com.ar/compartir/biblioteca/INFOSEC/Mitnick%20Kevin%20-%20El%20Arte%20De%20La%20Intrusion.PDF

MITNIK Kevin, El arte de engaño, 2001 [En línea], disponible en http://www.seaceptanideas.com/biblio/El_Arte_del_Enga%C3%B1o.pdf

MONTERO David, Ingeniería Social, [En línea] OWASP, 2007, disponible en https://docplayer.es/15753809-Owand-11-granada-ingenieria-social.html

MORALES José Ph.D. Ingeniería Social, [En línea], España: Instituto Nacional de Ciberseguridad Cibercamp 2014, {30 septiembre de 2017}, disponible en https://cybercamp.es/cybercamp2014/attachments/multimedia/CyberCamp_IngenieriaSocial.pdf

NAVARRO Antonio, Como evitar ser víctima de la ingeniería Social: consejos útiles, [En línea], 2011, disponible en http://www.ticsconsulting.es/blog/generar-claves-seguras-3

OWASP LatamTour, Ingenieria Social: Hacking Psicologico [En línea], 2016 Republica dominicana, disponible en https://www.owasp.org/images/2/27/02_INGENIER%C3%8DA_SOCIAL.pdf

PANDA SECURITY, CryptoLocker: Qué es y cómo evitarlo, [En línea] 2015, disponible en https://www.pandasecurity.com/spain/mediacenter/malware/cryptolocker/

PAGNOTTA Sabrina, Las 5 historias de Ingeniería Social más ridículas de los últimos tiempos [En línea], ESET, 2015, disponible en: https://www.welivesecurity.com/la-es/2015/12/01/historias-de-ingenieria-social-ridiculas/

PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA, Directiva (UE) 2016/1148, [En línea], de 6 de Julio de 2016, Disponible en: https://www.boe.es/doue/2016/194/L00001-00030.pdf

PISCITELLI Emiliano. Ingeniería Social: Cuáles son los tipos de ataque. [En línea], RedUSERS. 2015, Disponible en http://www.redusers.com/noticias/ingenieria-social-cuales-son-los-tipos-de-ataque/

RANCHAL Juan, Robo de datos bancarios en Android por ataques de ingeniería social, [En línea], 2012, disponible en https://www.muyseguridad.net/2012/03/16/robo-datos-bancarios-android-ataques-ingenieria-social/

SANTIAGO Sarah, Ingeniería social, cuando blindar sistemas informáticos no lo es todo [En línea] Seguridad Informática para Todos, 2017, disponible en https://opendatasecurity.io/es/ingenieria-social-cuando-blindar-sistemas-informaticos-no-lo-es-todo/

SHACKLEFORD, Dave. Pruebas de penetración en ingeniería social: cuatro técnicas efectivas, [En línea], TechTarget. 2012, Disponible en: https://searchdatacenter.techtarget.com/es/consejo/Pruebas-de-penetracion-en-ingenieria-social-cuatro-tecnicas-efectivas

SYMANTEC, ¿Qué es el smishing?, 2017, NORTON COLOMBIA, Disponible en: https://co.norton.com/internetsecurity-emerging-threats-what-is-smishing.html

THE HACKER NEWS, Dyre Wolf roba más de 1 millón de dólares por transacción, [En línea], 2015, Disponible en: https://www.seguridad.unam.mx/historico/noticia/index.html-noti=2216

TORRES Alissa, Ingeniería Social, México: Securing the human SANS, 2014.

TREND MICRO, 5 Motivos por los que las trampas de la ingeniería social funcionan. [En línea], 2012, Disponible en: http://www.trendmicro.es/media/br/5-reasons-why-social-engineering-tricks-work-es.pdf

YEBOAH Ezer & MATEKO Priscilla. Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices, Journal of Emerging Trends in Computing and Information Sciences. [En linea], 2014, Disponible en: https://pdfs.semanticscholar.org/7a27/1a3ff90b2a19d6b4f4ecc800e0aebdcda063.pdf

ZOTTO Rodolfo S. "Spam" o correo electrónico no deseado, Editorial ASTREA, pp2, [En línea], 2004, Disponible en: https://www.astrea.com.ar/resources/doctrina/doctrina0140.pdf