UNA BREVE MIRADA A LA INGENIERIA SOCIAL

Camacho Nieto, Nelson Andrés.
andres_c_@hotmail.com
Universidad Piloto de Colombia

Resumen— La presunción de que hurto informático, ataque o hackeo corporativo y/o personal solo ocurren a grandes emporios o personas acaudaladas, es un error común; la verdad es que hoy en día este tipo de ataques, se dan de la manera más absurda e ingenua y la verdad en la mayoría de los casos no se nota cuando se entrega información confidencial o cómo se facilita el acceso a nuestra data. El presente escrito muestra y/o da a conocer un análisis sobre la ingeniería social, permitiendo vislumbrar las técnicas utilizadas para persuadir a los demás en tomas de decisiones que conlleven a la obtención de datos relevantes del objetivo, así como su evolución y premisas utilizadas en el mundo de la world wide web, queriendo denotar que aun a pesar de tener el termino social en su nombre, no solo se limita la interacción persona a persona, sino que va mas allá; llegando a instar al objetivo (persona) a dar información a través de la tecnología valiéndose de engaños y aprovechándose de la condición básica del ser humano de confiar en que ve o no ver más allá de lo que se le presenta o se le muestra.

Índice de Términos— información confidencial, manipulación, ataque, ingeniería social.

Abstract - The presumption of which computer robbery, attack or hackeo corporate and/or alone personnel they happen to big centers or wealthy persons, is a common error; the truth is that nowadays this type of attacks, they happen in a most absurd and ingenuous way and the truth in most cases is not evident when confidential information is delivered or how the access to our byline is facilitated. The written present shows and/or announces an analysis on the social engineering, allowing to glimpse the skills used to persuade to the others in captures of decisions that they bear to the securing of excellent information of the target, as well as its evolution and premises used in the world of the web world wide, queriendo to denote that even in spite of having the social term in its name, not only limits the interaction presents itself to person, but it goes further away; going so far as to urge to the target (person) to give information across the technology using of tricks and taking advantage of the basic condition of the human being to trust that it sees or not to see beyond what it appears before him or one shows him.

I. INTRODUCCIÓN

Siendo la información un bien invaluable, se gastan innumerables recursos en su protección; sin embargo, hay un activo que no se ha logrado proteger por completo; el hombre; y dada su complejidad, se convierte en un elemento voluble y difícil de blindar ante amenazas sociales.

Ahora bien; adentrándonos en el tema que nos atañe; *"La Ingeniería Social es el acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas. Éstas contemplan entre otras cosas: la obtención de información, el acceso a un sistema o la ejecución de una actividad más elaborada (como el robo de un activo), pudiendo ser o no del interés de la persona objetivo."*[1] Es decir, que la ingeniería social se podría definir como el arte del engaño.

Ahora bien; remontándonos en la historia y dentro de lo que se puede constatar como uso de la ingeniería social, nos encontramos con casos, que sin el ánimo de querer caer en lo jocoso e irrisorio han sido documentados desde las citas Bíblicas. Uno de tantos, podría ser la historia de Sansón y Dalila, en el cual Dalila haciendo uso de sus atributos y belleza logro engañar a Sansón, haciendo que este le revelase el origen de su fuerza; esto lo hizo sin que Dalila tuviese que recurrir a métodos violentos o invasivos; y como este hay muchas citas más.

Este es un ejemplo claro de cómo la ingeniería

[1] Extraído de http://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

social influye en la toma de decisiones de los demás logrando manipular de manera pasiva a un individuo para obtener información requerida.

Ahora bien; como la idea es no abstraernos de la realidad, en la actualidad, se tiene que sus orígenes propiamente dichos datan de la década de los 90's y fueron implantados por Kevin Mitnick – también conocido como "Cóndor", considerado como uno de los mejores hackers de la historia, quien realizo la mayoría de intrusiones gracias al uso de teléfonos, extrayendo información relevante de sus interlocutores, y quien ahora se desempeña como consultor de seguridad. Según Mitnick *"la ingeniería social es posible por la explotación de 4 aspectos básicos inherentes al ser humano:*

1. *Todos queremos ayudar.*
2. *El primer movimiento es siempre de confianza hacia el otro.*
3. *No nos gusta decir no.*
4. *A todos nos gusta que nos alaben."*[2]

Estas premisas permiten de alguna manera aprovechar las falencias de la condición humana para idear una estrategia que permita influir sobre la toma de decisiones de las personas; el hecho de ser confiados y tener la necesidad de dar más información de la requerida, permite lograr captar información relevante sin habernos dado por enterados.

Cabe notar que el termino falencia se usa, dadas las actuales condiciones psico-sociales en los cuales se desenvuelve la humanidad, y que han desarrollado técnicas en las cuales, el dar confianza o información a "X" individuo, puede resultar contraproducente.

Así mismo, y con el pasar de los tiempos y los avances tecnológicos sumados al agitado ritmo de vida han evolucionado, permitiendo que estas premisas se amolden a condiciones acorde al entorno virtual.

Dentro de las premisas de perpetración que tienen los cyber-delincuentes, se hace uso de algunas características básicas de todo usuario normal de internet. Tales premisas son:

Curiosidad: esta premisa hace referencia al acceso a sitios que denotan accesos prohibidos, con contenido explícito o mails que hacen referencia a videos o fotos de alguna celebridad. Al acceder a estos mails o links, se puede implantar un código malicioso en el pc logrando tener acceso en Segundo nivel.

Atracción: se ve comúnmente en redes sociales y mails; la idea de esta táctica es suplantar identidad de alguna mujer con grandes atributos y enviando correos de contacto o solicitudes de Amistad a redes sociales, entablando conversaciones con el ánimo de ganar la confianza del objetivo. Una vez el target se siente confiado se pueden extraer datos requeridos para el atacante.

Miedo: este medio de perpetración cuenta con 2 fases; en la primera, se usa mas comúnmente vía mail; la idea es como su nombre lo indica, generar miedo y/o incertidumbre a los objetivos haciendo alusión a violación de datos confidenciales, ayudas o auxilios económicos; en la segunda, envían links de acceso en los cuales pueden realizar supuestos cambios de clave y/o códigos de acceso a cuentas bancarias o de correo, extrayendo de esta manera información requerida.

Este tipo de perpetración también se usa como medio extorsivo, en el cual envían capturas de pantalla del objetivo mostrando evidencia de uso indebido de los recursos tecnológicos asignados y se solicita una paga para no difundir la información.

Empatía: este método consiste en apelar a las buenas acciones por medio de correos alusivos a personas con enfermedades terminales u obras caritativas, solicitando auxilios económicos por transferencia o consignación directa o en su forma más avanzada, la simple solicitud del reenvío de la información a X cantidad de amigos hasta localizar la información requerida o acceso al objetivo.

De acuerdo a las premisas y características de explotación, se evidencia que el arte de la ingeniería social está evolucionando constantemente y va a la par con los avances tecnológicos, llevándonos a un

[2] OWASP Education Proyect; Montero Abujas David.

punto de quiebre en el cual la tecnología de uso cotidiano y personal se ha vuelto en nuestra contra por la falta de conocimiento y la necesidad de publicar nuestro quehacer diario en redes sociales, fotos y demás.

Si bien es cierto que las oportunidades para perpetrar un ataque a este nivel se basan en falencias propias, también hay que correlacionar los cambios socioculturales y los avances tecnológicos, los cuales, aunados con la necesidad de estar en la vanguardia tecnológica, dan pie a generar brechas de seguridad tanto personal como empresarial.

La ingeniería social en este contexto no es más que el arte de hackear al individuo; es decir, que ya no solo se Hackean equipos de cómputo, redes y empresas, sino que también se Hackean personas; pero, ¿porque la efectividad de esta técnica?; pues bien, su efectividad reside en la confianza y en el exceso de confianza que tenemos para comunicarnos, sumándole a ello, la falta de información en el tema.

II. ¿CÓMO NOS AFECTA Y PORQUE SOMOS TAN VULNERABLES?

De acuerdo a EC – Council, "*"La ingeniería social no es una técnica cuadriculada. Depende de la malicia del atacante, así como de la que tenga la víctima. Se pueden utilizar infinidad de argucias y mañas para lograr la información que se necesita: desde sobornos a amigos y familiares para que faciliten el acceso a ella, hasta preguntas sueltas en ambientes de esparcimiento, correos electrónicos aparentemente inofensivos que hacen preguntas sencillas y cuyas respuestas interesan a quien solicita la información"*, sostiene la ingeniera Jacqueline Tangarife, gerente de Security Solutions & Education, empresa que es la representante exclusiva para Colombia de EC-Council Academia."[3]

Estando en pleno siglo XXI, las condiciones de activos de valor han cambiado notablemente, siendo hoy en día, la información el bien más preciado para las corporaciones, entidades, organizaciones, empresas y personas.

Una pérdida de información, plagio, secuestro o hurto de la información supone un impacto directo a la credibilidad, a la continuidad del negocio y en caso de ser perpetrado a un individuo, a su autoestima; la tecnología comprometida se puede restaurar; sin embargo, la pérdida de la data o la información, es un fuerte golpe para cualquier entidad y/o persona. ¿Pero porque se habla de ingeniería social no solo a nivel de individuo, sino que ha trascendido a nivel empresarial? La respuesta radica en las condiciones en las cuales se trata la información, y la inclusión de un nuevo termino; *"datos en movimiento"*[4]. Este término hace referencia a la relación que guarda la tecnología y la data; dicho de otra manera, hace referencia a la capacidad de mover información sea personal o empresarial en elementos de uso diario como tabletas, Smartphones, portátiles y demás, así como también la necesidad de la disponibilidad de la misma, lo que genera desarrollos que permiten acceder a ambientes empresariales desde estos elementos; es lo que se denomina la oficina móvil.

Según información revelada en el CPMX2 por David Shekaiban, al año se reportan más de 12000 equipos de cómputo como perdidos en cerca de 200 terminales aéreas alrededor del mundo, lo que supone perdida de información corporativa y personal.

Lo anterior nos lleva a un escenario de cuestionamientos acerca de las condiciones de seguridad de nuestros datos sean personales o corporativos.

- ¿En espacios abiertos tenemos la precaución de verificar las condiciones en las cuales accedemos nuestros equipos? ¿Alguien ve nuestras claves?, observan nuestra pantalla cuando ingresamos a redes sociales, cuentas de correo y demás? ¿Tenemos nuestros equipos celulares protegidos y la data debidamente asegurada? ¿Las personas que nos conocen, que tanta información nuestra revelan? ¿Con que facilidad lo hacen? ¿A nivel corporativo que medidas de control se tienen para con los contratistas y terceros? ¿se tienen establecidos

[3] Extraído de http://www.enter.co/guias/tecnoguias-para-empresas/ingenieria-social-el-hackeo-silencioso/

[4] David Shekaiban, conferencia CPMX2 - .2010

acuerdos de confidencialidad? ¿Se tienen medidas de control y protección de la data cuando se requiere soporte a equipos de cómputo? ¿Se tienen políticas en cuanto a la apertura de e-mails de cuentas desconocidas? ¿Ejecución de archivos adjuntos? ¿Se sabe cómo validar un remitente?

Estos cuestionamientos tienen su fundamento en el hecho de que en ellas se reflejan las amenazas y vulnerabilidades a las cuales nos vemos expuestos con mayor frecuencia y son tan comunes que se pierde el sentido de alerta para con estas premisas; sin embargo, su desconocimiento trae consigo consecuencias como por ejemplo la ejecución de un ramsomware como cryptolocker, Phising, robo de credenciales, entre otras.

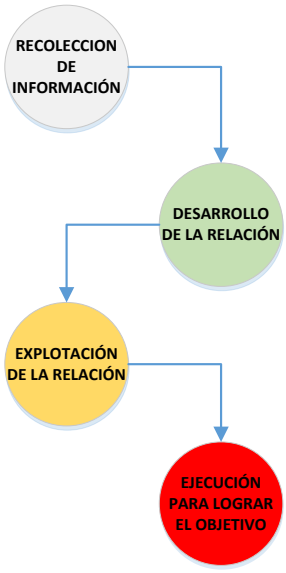
Lo anterior nos permite inferir que las malas prácticas y la confianza excesiva, proporcionan vectores de ataque que abren posibilidades de acceso y múltiples puntos de ingreso, lo que nos lleva a reafirmar el hecho de que el ser humano es el eslabón más débil de la cadena.

La página de TrendMicro – www.trendmicro.es, informo que el acceso a links no confirmados permitió que, para el día de san Valentín, en publicidad alusiva a esta fecha, se descargara código malicioso en navegadores como Chrome y Mozilla Firefox. Es por esto que el simple hecho de contar con un acceso a internet, tener cuentas de correo y redes sociales ya nos hacen un blanco para cualquier ataque de ingeniería social; no con esto se quiere decir que se debe limitar o evitar el acceso a recursos tecnológicos; basta con tener conciencia sobre el correcto uso del internet y evitar caer en trampas con nombres llamativos como premios, rebajas o solicitud de cambio de claves vía mail.

De acuerdo a la guia de TrendLabs (TrendMicro) “5 motivos por los que las trampas de la ingeniería social funcionan”, se hace referencia al hecho de que *“Las amenazas de ingeniería social son peores que el malware más intrusivo, ya que es más difícil protegerse frente a ellas. ¿El motivo? El objetivo es usted, no simplemente su sistema”*.[5] Invita a la necesidad imperativa de mantenerse informado y tener capacitaciones constantes o promulgar las condiciones sobre las cuales se presentan estos ataques; definir las condiciones sobre las cuales se da un ataque de este tipo, como identificarlo y qué hacer si se es víctima de uno de ellos.

¿Qué funcionario de TI no ha tenido que asesorar a algún funcionario de X entidad sobre un correo electrónico con mensaje extraño en el que se hace referencia a la urgencia de abrir mensaje con archivo adjunto? ¿Apartándonos del ambiente empresarial, en su hogar no ha tenido dudas al respecto? Si alguna vez hemos recibido este tipo de solicitudes de apoyo, nuestra entidad está en riesgo inminente; se evidencia la necesidad de crear campañas informativas sobre este tema y el presente documento, puede ser un buen punto de partida; pero, ¿cómo puede afectar un ataque de ingeniería social? Para entender esto se debe tener en cuenta que cualquier tipo de ataque consta de una serie de pasos y/o etapas necesarias para lograr extraer información necesaria para explotar las vulnerabilidades encontradas que permitan lograr el objetivo. Es decir que todo ataque o ptest (prueba de penetración), cuenta con un ciclo, el cual para esta temática se denomina ciclo de ataque de ingeniería social ver figura 1.

Figura 1.



Ciclo de ataque de ingeniería social.

Fuente: el autor.

[5] Extraído de http://www.trendmicro.es/media/br/5-reasons-why-social-engineering-tricks-work-es.pdf

La afectación generada por dichos ataques, radica en la condición humana; si, aunque suene raro, es esta condición la que nos lleva a ser presa fácil de los atacantes ya que se aprovechan del hecho de siempre querer colaborar de más, ser comunicativos, confiar en los demás y más aún, de la ignorancia en el tema. Lo irónico es que, en estos tiempos de virtualización de las relaciones interpersonales, no se genera conciencia sobre este tema ni siquiera al interior de las casas y hogares, y mucho menos con hijos y colegios. Se debe tener especial atención con el hecho de que esto no es tema exclusivo de empresas o entidades; todo individuo susceptible a ser explotado económicamente es vulnerable y objetivo de dicha técnica.

III. TÉCNICAS Y TIPOS DE ATAQUE

Ahora bien; luego de todo lo anteriormente expuesto en lo que respecta a la ingeniería social, es hora de abordar la explotación de vulnerabilidades o consecuencias de no tener en cuenta condiciones básicas y/o mínimas de seguridad para evitar un ataque de ingeniería social. Para esto debemos entender los tipos de ataque de ingeniería social:

1. **Engaño Humano:** interacción directa con el objetivo o quien tiene acceso a este. Es aquí donde las dotes de manipulación sobresalen y el ataque se da a nivel psicológico.

- **Hunting:** ataque bajo perfil, no se tiene interacción completa con el objetivo y esta se limita a un par de veces nada más. La información aquí conseguida se usa en ataques directos tipo Phising en el que previo contacto se hace creer al objetivo que se forma parte de una entidad, organización o conocido, instando a la víctima a que inserte datos personales en una url supuestamente real.

- **Farming:** la exposición es prolongada con el fin de extraer la mayor cantidad de información y obtener la mayor cantidad de datos relevantes sobre el objetivo del ataque. De alguna manera aquí la idea es ganar la confianza de la víctima.

- **Dumpster diving:** recolección de información por medio de la basura. Lamentablemente se tiene la costumbre de no destruir correos, estados de cuenta y demás información que para alguien puede tener valor. Se pueden conseguir números telefónicos, cuentas de correo, direcciones y demás que permiten perfilar de mejor manera al objetivo.

2. **Engaño basado en tecnología:**

- **Phising:** envío de mail con el fin de instar a la víctima a que por medio de un link o un formulario envíe datos personales o corporativos; (suplantación de identidad). Para este tipo de ataque, y como se puede observar en la figura 2, el atacante sigue 5 pasos básicos para completar el circuito del ataque.

Paso 1 – falsificación de un ente de confianza. Es decir, un contacto o entidad que genere confianza.

Paso 2 – envío de mensajes por algún medio de propagación. En este punto el atacante establece el tipo de repliegue de información que va a hacer por medios electrónicos.

Paso 3 – Un porcentaje de usuarios confía y da click en el mensaje enviado previamente.

Paso 4 – al dar click en el mensaje se abre una página web falsa en la que los usuarios ingresan sus datos.

Paso 5 - el atacante obtiene los datos personales y es libre de usarlos a su conveniencia. Ver figura 2.

Figura 2

Circuito de un ataque – Phising.

Fuente: http://www.pcworld.com.mx/UserFiles/File/Eset-infografia-phishing%20(1).png

- **Correo spam:** correos con publicitarios, información falsa, accesos a sitios de citas y demás que luego de dar click a un link, se descarga una

aplicación que permite acceso al atacante.

- **Software:** se envían ventanas solicitando instalar programas o actualizaciones con ciertos beneficios pero que en segundo plano pueden estar instalando un keylogger, por ejemplo, entre otros.

Este tipo de ataques e incursiones se ven desde colegios hasta grandes corporaciones, sin distingo regional ni fronterizo; es más; la proliferación de redes sociales personales como laborales como LinkedIn, permiten a un atacante realizar un estudio previo y un perfil de su objetivo; datos como números de celular, contactos, área de trabajo, nombre de la entidad, permiten ver que tan atractivo es el individuo con respecto al objetivo final.

¿Pero porque algo que esta tan de moda o que en cierta medida es una herramienta necesaria para darse a conocer o tratar con clientes, puede resultar contraproducente? La respuesta está en la forma como se asocia la información a estas herramientas, pasando por alto los perfiles de seguridad; es decir, publicamos información sin perfilar su privacidad; a esto se le suma la interacción que tienen las aplicaciones móviles con las redes sociales y como estas "generan" la necesidad de extraer datos de las redes sociales para visibilizar y replicar la información requerida, pero usando información no requerida sin que nos demos cuenta de ello.

Es tan común hoy en día el uso de herramientas tecnológicas de comunicación como WhatsApp que no se toman las debidas medidas de protección en lo que respecta a envío y recepción de archivos, dentro de los cuales se pueden enmascarar aplicaciones nocivas para nuestros dispositivos móviles y permitiendo de manera desinteresada relación de contactos con otras redes como sucede desde hace no más de 15 días con Facebook, en donde se informa de la necesidad de correlacionar la información de contactos entre estas 2 grades redes sin permitir declinar las condiciones de acuerdo a las condiciones de privacidad de los usuarios.

Lo anterior se enmarca en las condiciones o factores de riesgo que se tienen al manejar información corporativa en redes sociales. *"Una de las principales desventajas del uso de las Redes Sociales es el desconocimiento de las políticas de privacidad y el mal uso por parte de las empresas, de sus empleados y directivos. Esto representa enormes riesgos de filtrar información confidencial en las Redes Sociales. En la actualidad las diferentes empresas de Redes Sociales han estado cambiando constantemente los términos y condiciones de uso y privacidad, y la mayoría de los internautas desconocen y no están conscientes de estos cambios, trayendo consigo riesgos importantes en la privacidad de individuos y empresas."*[6]

Claro está que se puede romper este vínculo, pero muchas veces se da click en cuanta ventana aparezca sin verificar su contenido.

Lo que es cierto, es que la vida privada y personal paso a un segundo plano siendo esta casi inexistente, ya que en internet se puede localizar información de cualquier persona permitiendo desplegar una serie de herramientas para extraer información más detallada facilitando ataques de ingeniería social.

"Según Andrés Galindo Director de Negocios y Alianzas Estratégicas de Digiware de la identificación de la víctima se desprende un sin número de métodos. Uno de ellos es el envío de "malware modificado" a través de correo electrónico, en el que el delincuente sabe con anterioridad el sistema de seguridad o antivirus, cumpliendo con el objetivo de acceder a los datos de la compañía. "S*i se sabe que una pared impide ingresar a un computador físicamente, entonces la alternativa es infiltrarse virtualmente. Si el delincuente conoce de manera previa datos como correo, tipo de antivirus en el ordenador, número de celular entre otros datos del sujeto estudiado, le será más sencillo infiltrarse sin el consentimiento de la víctima en cuestión".*

Para Digiware el concepto más básico en seguridad informática, gira en torno a que ésta es tan fuerte como el eslabón más débil de la cadena, "*el ser humano".* Así lo confirma el aumento de los ataques persistentes focalizados, puesto que en lo corrido del último año pasaron del 1% al 30% "*es preocupante este aumento, pues de*

[6] Extraído de http://socialwebmarketing.mx/desventajas-y-riesgos-de-las-redes-sociales-en-las-pymes/

antemano se sabe que estos ataques exigen al delincuente en cuanto a Ingeniera Social, un estudio previo y una preparación del objetivo o foco", puntualizó Galindo."[7]

Lo anterior no es otra cosa más que una validación de la relación directa que existe entre los avances tecnológicos, la proliferación de redes sociales y publicación de información, con la vulnerabilidad a ataques de ingeniería social y a su vez con el aumento de ataques de este tipo, máxime aun cuando el vector de ataque se da en ambiente tecnológico lo cual expande las posibilidades de conseguir información y correlacionar esta con el objetivo. Irónicamente la página *http://muyseguridad.net/2013/10/09/estafas-correo-electronico/* muestra un top 10 de las estafas más usadas a través de e-mail, y aquí se ven tipologías de correos spam que aun hoy día circulan tanto en cuentas corporativas como en correos personales. Lo anterior denota no la falta de evolución en estos ataques, sino su efectividad y valides aun a pesar del tiempo. Cabe resaltar que los más utilizados hoy en día es la suplantación de identidad (phishing) y los correos spam que denotan o bien información socio-jurídica o publicidad; estos correos tienen como característica principal el requerir información o respuesta urgente para notificaciones judiciales.

La idea de compilar esta información radica en la necesidad de dar a conocer las condiciones a las cuales nos enfrentamos día a día en lo que respecta al tratamiento de la información; es básicamente, salvaguardar los intereses personales y corporativos, dentro de los cuales el que puede tener mayor valor es la información. Para esto, una de las estrategias planteadas es capacitar y concientizar a TODOS los usuarios y/o funcionarios de la entidad sobre lo que es o son los ataques de ingeniería social, características, usos, modalidades, así como la importancia de tener y manejar privilegios de acceso acorde a las funciones que se desempeñan; pero sobre todo la importancia de manipular de manera adecuada la información confidencial.

IV. ¿PERO CÓMO PROTEGERNOS ANTE UNA EVENTUAL INTRUSIÓN O ATAQUE DE INGENIERÍA SOCIAL?

- Como primera medida, INFORMACION; se debe tener informada a la comunidad sobre dichas amenazas, como funcionan, como reconocerlas y establecer canales de comunicación adecuados que permitan reportar dichas irregularidades.
- A nivel corporativo se debería fijar una política que defina canales de comunicación, reporte, que se puede y que NO se puede hacer en los equipos de cómputo, así como fijar políticas de uso de correo e internet; sin embargo, esto no sirve de nada si no se hace una jornada de capacitación y/o concienciación sobre este tema.
- No todo documento en físico que ya no se requiera independiente a la razón que sea, se debe reciclar o dejar en cajas para reutilización; en ocasiones la información que alguna vez fue sensible contiene datos que si bien es cierto a nuestra entidad ya no le es útil, otras personas si pueden extraer datos relevantes para fijar o perfilar objetivos; es por esto, que se recomienda destruir dicha información.

Ahora bien; el hecho de que gran parte de este trabajo se haya encaminado a la parte corporativa no quiere decir que sus preceptos no apliquen en la cotidianidad de todo individuo con capacidad de comunicación. Sus condiciones solo se fijan en lo atractivo del objetivo; en que se puede extraer y que beneficio comúnmente económico se puede lograr de un ataque en este nivel; es por esto que no está demás recalcar el hecho de que todos somos posibles objetivos; seamos empleados, empresarios, estudiantes, etc. La información es tan valiosa como el uso que le demos a esta; no se debe echar en saco roto los acontecimientos de hurtos por redes sociales, acoso, hurto a residencias por suplantación de identidad y el hecho de que todo esto se da o se puede evitar con el uso y manejo que se le dé a la información.

[7] Extraído de ACIS: http://www.acis.org.co/portal/content/ingenier%C3%ADa-social-el-primer-paso-para-las-vulneraciones-en-seguridad-inform%C3%A1tica

V. CONCLUSIONES

La ingeniería social no solo debe entenderse como una amenaza a nivel tecnológico; por su origen y necesidad de obtener información, el simple hecho de dar confianza al punto de brindar información personal ya nos hace vulnerables; es por esto, que día a día más entidades de diversas áreas están volteando sus ojos a minimizar los riesgos de sabotaje o vulneración de seguridad al interior de sus redes y sistemas apostando al cierre de brechas que permitan permear el perímetro de seguridad de la entidad. La medida más eficiente para tratar de poner freno a esta situación es informar a nuestros compañeros, colaboradores y amigos sobre los riesgos a los cuales nos vemos expuestos por no manejar unos parámetros mínimos de "confidencialidad".

Cabe notar que esto no solo aplica para la vida laboral; también es bueno realizar actividades de concienciación en casa y sobre todo con menores de edad quienes hoy en día son susceptibles a suplantación de identidades en las redes sociales, en las cuales además de todo no manejan parámetros mínimos de privacidad, llevándolos a publicar su vida como si fuese un diario, incluyendo datos personales como de ubicación actual, gustos y demás. Tal es el manejo de información en esta red que se puede hacer un perfil detallado de las personas solo navegando por las redes sociales o buscando por nombre propio en los buscadores de internet.

"La información que damos acerca de nuestra vida diaria en las redes sociales es mucha, y cada vez más. Quizás en muchos casos sea demasiada. Pero… más allá de la pérdida de privacidad que muchos usuarios de estas plataformas asumen en pro de las ventajas que conllevan, ***el uso de las redes sociales o, mejor dicho, contar demasiadas cosas de nosotros mismos en estos sistemas conlleva riesgos de seguridad importantes****,… La ingeniería social, el robo de identidades, el ciber-acoso… son solo algunas de las amenazas que proliferan al calor de estas plataformas. Saber qué debemos contar y cómo es clave para nuestra seguridad."*[8]

Un error común, es el pensar que la información confidencial, sea personal o corporativa, solo se puede extraer al ser víctimas de ataques cibernéticos. En términos generales, la extracción de información por este medio, se da gracias a las malas prácticas de uso de los sistemas de comunicación o la capacidad de develar información a personas ajenas sin siquiera percatarnos de ello. Lo absurdo de esto es que nuestra formación nos da la capacidad de poder movernos en el mundo sin romper reglas básicas como hablar con extraños, dar información personal o privilegiada a desconocidos entre otras.

A nivel corporativo y Teniendo en cuenta el crecimiento exponencial de estas técnicas en la captación ilegal de información para fines maliciosos, el mundo ha fijado su mirada en la implementación de sistemas de gestión de riesgos de la información y en la implantación de políticas de seguridad informática que mitiguen los riesgos a los cuales están expuestas las entidades por ataques de este tipo. A nivel de otros espacios ajenos a la vida laboral, hasta ahora se están viendo tímidos esfuerzos encaminados a concienciar sobre el uso de la información; lo que se debe o no publicar en redes sociales y que tanta información se devela de manera inconsciente.

El mundo real como se puede ver no siempre es tan complejo como quisiéramos verlo; sin embargo, el hecho de ser confiados y en cierta medida confiables afecta nuestras relaciones interpersonales dando espacio a hablar más de lo que se debe o de lo que se quiere; sin embargo, su homólogo digital si lo es; nos disparan ofertas engañosas, correos de destinatarios aparentemente conocidos, links de acceso que a simple vista son reales y verificables, redes sociales en constante crecimiento y evolución, la deshumanización de las relaciones interpersonales entre otros factores nos lleva a ser realmente vulnerables; a no medir los actos aparentemente inocentes y por ende a no medir consecuencias.

[8] Extraído de http://www.ticbeat.com/socialmedia/los-riesgos-de-publicar-demasiada-informacion-personal-en-las-redes-sociales/

Ya no somos solamente un numero en un documento; ahora somos un mar de información en red. Se nos puede localizar, seguir, hablar, ver, conocer e interactuar sin limitaciones de distancia. Es por esto que su valor es deslegitimizado por causa del desconocimiento.

El desarrollo del presente escrito no pretende generar alarmas al punto de volver paranoica a la sociedad en cuanto al uso de información, equipos de cómputo, internet, redes sociales o frente a la interacción con otro individuo; sin embargo, si se pretende generar alerta frente a lo que se hace en la cotidianidad, la información que se comparte, la que se publica y la que se da a terceros. La intención en concientizar sobre el correcto uso de las TIC´s, y la interacción con desconocidos; generar conciencia de la importancia de tratar estos temas al interior de los hogares, colegios y empresas y su masificación. Es evidenciar que la problemática es latente y que la corresponsabilidad obliga a actuar, informando y educando máxime cuando es la información y su uso sea personal o no ya forma parte de la cotidianidad; esta va desde oficinas móviles y teletrabajo hasta la necesidad de publicar y existir en el ciber mundo, donde se dice que quien no está en internet, sencillamente no existe.

VI. REFERENCIAS

[1] Abujas, D. M. (2007). *The OWASP Foundation*. Obtenido de The OWASP Foundation: http://osl.ugr.es/descargas/OWAND11/OWAND11%20Granada%20-%20Ingenier%C3%ADa%20social.pdf

[2] Andrés Galindo. (Julio de 2016). *ACIS*. Obtenido de ACIS: http://www.acis.org.co/portal/content/ingenier%C3%ADa-social-el-primer-paso-para-las-vulneraciones-en-seguridad-inform%C3%A1tica

[3] Castellanos, E. J. (4 de Mayo de 2011). Ingeniería Social: Corrompiendo la mente humana. Mexico.

[4] Ingeniera Jacqueline Tangarife. (s.f.). *http://www.enter.co/*. Obtenido de http://www.enter.co/: http://www.enter.co/guias/tecnoguias-para-empresas/ingenieria-social-el-hackeo-silencioso/

[5] Shekaiban, D. (2010). *Expresion Binaria.* Obtenido de Expresion Binaria: http://www.expresionbinaria.com/campus-party-seguridad-informatica-y-analisis-forense/

[6] *Social&web marketing*. (2015). Obtenido de Social&web marketing: http://socialwebmarketing.mx/desventajas-y-riesgos-de-las-redes-sociales-en-las-pymes/

[7] *ticbeat*. (17 de Septiembre de 2013). Obtenido de ticbeat: http://www.ticbeat.com/socialmedia/los-riesgos-de-publicar-demasiada-informacion-personal-en-las-redes-sociales/

[8] *trendmicro.* (2012). Obtenido de trendmicro: http://www.trendmicro.es/media/br/5-reasons-why-social-engineering-tricks-work-es.pdf