# INGENIERÍA SOCIAL, UNA TÉCNICA SUBESTIMADA POR DESCONOCIMIENTO

Sánchez Patarroyo, Henry.
henryszp@gmail.com
Universidad Piloto de Colombia

***Resumen—***¿Cómo se llama tu mascota?, ¿cuál es tu película favorita?, ¿cuál es el nombre de tus hijos, de tus sobrinos de tus padres, etc.?, preguntas como estas pueden darse en una conversación esporádica o estar publicadas en alguna red social; información que se expone sin tener en cuenta la connotación que pueda llegar a tener. Preguntas tan básicas como estas son las que algunos programas de las compañías solicitan como método para identificar un usuario y posiblemente restaurar una clave; procedimiento que muchas personas pasan por alto y no le prestan la atención ni importancia respectiva. Otras situaciones pueden ser más complejas pero de igual manera imperceptibles ante el verdadero objetivo, un correo no esperado con información que despierta la curiosidad, temor o interés por algún evento; un papel desechado o una conversación importante que posiblemente alguien este escuchando sin ser detectado. Estas técnicas que se pueden llegar a mezclar con la rutina de las personas se pueden agrupar dentro de un contexto llamado ingeniería social, una técnica que se aprovecha del eslabón más débil de la seguridad de la información en cualquier ámbito, es decir, las personas y toma una fuerza considerable en esta era donde la información es un eje fundamental y lo trivial para algunos es un tesoro para otros, todo patrocinado por una gran consigna: desinformación.

***Índice de Términos—***Confianza, desinformación, ingeniería social, técnica.

***Abstract—***¿How is called your pet?, ¿what is your favorite movie?, ¿what is the name of your children, your nephews of your parents, etc.?, questions like these can occur in a sporadic conversation or be published in some social network; information that is exposed without taking into account the connotation that can get to have. Such basic questions as these are those that some programs of the companies request as a method to identify a user and possibly restore a key; procedure that many people ignored him and not pay attention or respective importance. Other situations can be more complex but equally imperceptible to the true objective; an email is not expected with information that arouses curiosity, fear, or interest in any event; a waste paper, or a conversation important that possibly someone this listening without being detected; these techniques that can be mixed with the routine of the people can be grouped within a context called social engineering; a technique that takes advantage of the weakest link in the security of the information in any scope, the people; and takes a considerable force in this era, where the information is a key axis and where the trivial for some is a treasure for others, and all sponsored by a great consignment: disinformation.

## I. INTRODUCCIÓN

Engaño, manipulación, halagos, empatía, métodos de convencimiento y persuasión son conductas humanas probablemente tan antiguas como la misma raza, técnicas y modos de comunicación e interrelación que se usaron desde tiempos remotos para conseguir objetivos específicos ya sea por sobrevivencia,

adaptabilidad, reconocimiento y aceptación entre otros. Con el paso del tiempo se perfeccionaron convirtiéndose en actividades más elaboradas como técnicas psicológicas y habilidades sociales, las cuales permiten manipular a las personas para que voluntariamente realicen actos que normalmente no harían. Existen varias perspectivas desde donde se puede abordar este actuar, situaciones tan naturales que no pretenden dañar como un vendedor que quiere dar a conocer su producto y se vale de adulaciones, carisma, manipulación y cierto tipo de presión para mantener a un usuario interesado, o como un niño el cual a través del llanto, rebeldía o por el simple amor de sus padres logra que en ocasiones accedan a sus caprichos. Innumerables situaciones como estas se pueden presentar dentro de la cotidianidad, sin embargo, este comportamiento y habilidades también pueden ser usados para realizar acciones que dañan directamente a algo o a alguien, partiendo de la obtención de información. Se aprovechan de las debilidades propias de las personas, como credulidad, ingenuidad, inocencia, ignorancia y todo esto sin que la víctima se percate, logrando comprometer desde una persona, hasta toda una organización. A estas técnicas y habilidades actualmente se les denomina como ingeniería social donde, hoy por hoy, es considerada una de las prácticas más poderosas y efectivas al momento de conseguir información sensible.

La información a través del tiempo ha tomado muchas más relevancia, tanto así que en 1979 Alvin Toffler, escritor y futurista estadounidense, publicó el libro llamado la tercera ola, donde da a conocer sus ideas acerca de la visión del estado social en el futuro describiendo en primera instancia el pasado y el presente y relacionando tres sucesos que involucran cambios significativos. La primera ola es la revolución agrícola, la segunda ola es la revolución industrial y la tercera ola es la sociedad del conocimiento y de la información. Aun a pesar del tiempo de su publicación los conceptos expresados en muchos aspectos son bastante actuales, llevándolo a realizar afirmaciones como: *"Un analfabeto será aquel que no sepa dónde ir a buscar la información que requiere en un momento dado para resolver una problemática concreta. La persona formada no lo será a base de conocimientos inamovibles que posea en su mente, sino en función de sus capacidades para conocer lo que precise en cada momento."*[1]

Si el objetivo es la información, esta puede ser recopilada por diferentes personas con diferentes metas, ya sea para ayudar o para realizar algún tipo de daño. Dentro de estas personas o comunidades que aplican la ingeniería social con conocimiento de las acciones que realizan se pueden encontrar los organismos gubernamentales como la policía, agencias de inteligencia, agencias privadas, delincuencia organizada, pentesters, hackers o particulares que desean conocer cierta información de alguien en especial. Si la situación a tratar se enfoca en el uso de la ingeniería social para realizar daños a terceros obteniendo beneficios podemos citar a uno de los grandes exponentes de la ingeniería social para estos fines, se trata de Kevin Mitnick, considerado el delincuente informático más perseguido por el FBI y conocido como el "Cóndor". Inició manipulando líneas telefónicas a una corta edad pero luego se interesó por la computación y la ingeniería social, este último fue el método más utilizado por Mitnick para tener acceso a los sistemas informáticos de manera ilegal en organizaciones gubernamentales y grandes empresas en los Estados Unidos.

Su experticia en este medio lo llevó a formular cuatro principios fundamentales, los cuales considera que son comunes a todas las personas, o a su gran mayoría:

- ✓ *"Todos queremos ayudar.*
- ✓ *El primer movimiento es siempre de confianza hacia el otro.*
- ✓ *No nos gusta decir no.*

[1] Toffler, A. (s.f.). Obtenido de http://jackelinemedinaarbi.blogspot.com.co/2011/02/reflexiones-sobre-la-tercera-ola-de.html

- ✓ *A todos nos gusta que nos alaben."*[2]

Luego de ser capturado, juzgado y cumplir su condena se dedicó a ser consultor de seguridad informática, estuvo presente en el 2001 en la conferencia anual RSA la cual se caracteriza por ser la más grande conferencia de seguridad de datos y criptografía en el mundo y plasmó a través de un artículo su sorpresa cuando en un evento de tal magnitud, importancia y renombre, donde se exponían las nuevas tecnologías de seguridad del momento, no se tocó el tema de ingeniería social. Comenta que al dar una vuelta por la sala logró ingresar en dos oportunidades a la sala de expositores sin que nadie le prestara demasiada importancia y si fuese una persona mal intencionada, lograría acceder a los equipos en busca de información sensible; esta situación le permitió inferir en la siguiente premisa; *"Si el objetivo es proteger la red, no se puede confiar en la tecnología por sí sola."*[3]

## II. TÉCNICAS DESARROLLADAS

Se ha oído decir algo como una computadora apagada es una computadora segura, si ese es el caso, el usuario toma un papel más relevante y convierte a la ingeniería social en una técnica idónea para recopilar la información que se quiere con un plus muy importante en la relación costo beneficio. Se pueden identificar cuatro (4) elementos importantes a la hora de usar la ingeniería social:

- ✓ Una persona que busca la información.
- ✓ Una persona incauta o inocente, que tiene la información.
- ✓ Técnicas, procedimientos y herramientas para encontrar la información.
- ✓ Un objetivo definido (lucro o causar daño).

Con esos aspectos definidos podemos hablar de algunas técnicas de la ingeniería social

### *A. Técnicas pasivas:*

Se basa en la observación y análisis del comportamiento del objetivo, evalúa la rutina diaria del mismo, crea un perfil psicológico aproximado, detecta hábitos de consumo, portales de consulta, etc.

### *B. Técnicas no presenciales*

Destaca el uso del teléfono, vishing, smishing, cartas, fax o correos electrónicos solicitando información.

### *C. Técnicas presenciales no agresivas*

Tales como shoulder surfing, dumpster diving y seguimiento a personas, entre otras.

### *D. Técnicas presenciales agresivas*

Extorsión, presión psicológica, suplantación de identidad o phishing, spear phishing, pharming.

Dentro de los métodos citados anteriormente y de los cuales son considerados los más utilizados por los ciberdelincuentes se encuentran:

Vishing: Es una práctica que involucra el uso del teléfono e ingenuidad de los usuarios y se puede aplicar en dos modalidades. La primera se realiza a través de una grabación específica donde engañan a la víctima para que acto seguido marque a un número sugerido. En la segunda una persona llama directamente a la víctima haciéndose pasar por un operador donde le responden con un guión muy similar al servicio telefónico de atención al cliente de una entidad y así generan credibilidad, generalmente suelen hacerse pasar por entidades bancarias. En cualquiera de sus dos modos sugestionan al usuario informando que es posible que haya sido víctima de un fraude, o se requiere que actualice una información o que se necesita resolver algún inconveniente con la cuenta y solicitan información correspondiente a usuarios, claves, números

[2] Mitnick, K. (s.f.). Obtenido de http://www.pandasecurity.com/spain/mediacenter/seguridad/ingenieria-social-empresas/

[3] Mitnick, K. (s.f.). Obtenido de http://www.securityfocus.com/news/199

de tarjetas, códigos de seguridad, fechas de vencimiento entre otros.

Smishing: Es una variante del phishing, donde los usuarios de telefonía móvil reciben mensajes de un remitente desconocido con textos intimidantes o atractivos, algunos informando que se han hecho compras por un monto específico con su tarjeta y es necesario que se comunique urgente al número adjunto en caso que no sean gastos autorizados y evitar el pago; cuando el usuario se comunica alarmado al número sugerido responde el atacante con un protocolo similar al del banco solicitando información confidencial para supuestamente cancelar la compra pero en realidad están completando el fraude. En otros casos el mensaje de texto indica que ha ganado algún premio o existe alguna oferta interesante, o alguna noticia de la actualidad que despierta la curiosidad del usuario y los incitan a visitar páginas web asociadas dentro del mensaje con el objetivo de redirigirlo a portales fraudulentos y obtener información personal, robar datos bancarios o infectar el dispositivo móvil con algún troyano.

Shoulder surfing: Es una técnica de observación básica que se usa bastante para la obtención de información confidencial, se puede describir como mirar por encima del hombro, tan sencillo como acercarse de manera cautelosa a un usuario y observar de manera detenida lo que teclea, o lo que visualiza en alguna pantalla o alguna nota que por descuido dejó expuesta con alguna clave, en algunos casos pueden usar binoculares o cámaras miniatura para observar datos de entrada, en otras ocasiones los desarrolladores ayudan a que esta práctica sea eficiente, ya que diseñan aplicaciones que al escribir la clave no la decodifican y es completamente visible, sitios como puntos de pago en tiendas, supermercados, gasolineras o cajeros en espacios abiertos que usen la modalidad de pago con tarjetas, son muy vulnerables a esta técnica ya que están muy expuestos.

Dumpster diving: Es la búsqueda de información valiosa en la basura. Para algunas empresas puede resultar una práctica muy riesgosa. Pueden llegar a parar allí documentos confidenciales, configuraciones, correos, memorandos, libretas telefónicas, manuales de procedimiento, formatos con membretes y en algunos casos más delicados, hardware obsoleto.

Phishing: Se usa para adquirir de forma fraudulenta información confidencial ya sea personal o financiera a través de mensajes de correo electrónico utilizando el factor miedo, el engaño y el desconocimiento, en donde se suplanta personas o empresas de confianza en una aparente comunicación electrónica verídica.

Es un tipo de ataque amplio y disperso en donde envían la información a numerosos usuarios para que, entre tantos, alguno ingrese sus datos y así lucrarse con el fraude, ver figura 1.

*Figura 1*


*¿Cuánto puede llegar a ganar un atacante?*
*Fuente: https://www.infospyware.com/articulos/que-es-el-phishing/*

Suelen incluir enlaces que redirigen a páginas web falsificadas usando nombres de organizaciones reconocidas, simulan que el correo electrónico del remitente sea de la compañía en cuestión, añaden logotipos y demás distintivos para dar confianza al usuario haciéndole creer que está en un sitio oficial para posteriormente solicitarle ingresar información sensible provocando robo de identidad, de datos confidenciales o llevar a pérdidas económicas.

Una técnica efectiva del phishing consiste en enviar dentro de los correos archivos adjuntos los cuales al descargarlos ejecutan software malicioso como los keylogger, el cual intercepta y guarda las pulsaciones realizadas en el teclado del equipo infectado para luego ser enviada o recogida y posteriormente utilizada.

Pharming: Al igual que el phishing, este se vale de la suplantación de portales web, la diferencia radica en que es mucho más difícil detectar el portal falso ya que no necesitan que el usuario interactúe con algún correo malicioso, su complejidad radica en que el atacante modifica el sistema de resolución de nombres en dominio (dns) y conduce al usuario a una página web falsa aunque este digite la verdadera de manera correcta en la barra de direcciones.

Spear phishing: A diferencia de phishing, que ataca a una gran población aleatoria, el spear phishing se centra en grupos u organizaciones específicas para robar propiedad intelectual, datos financieros, secretos comerciales, entre otros, es un ataque más enfocado y de igual manera usa el correo y la suplantación para lograr su objetivo de hacerse a la información.

## III. REDES SOCIALES

Para garantizar aún más la efectividad de las técnicas de ingeniería social y conseguir lo que se desea, el atacante recopila información personal de las víctimas y con esta diseña una treta o engaño más apropiado al lograr generar más confianza con información verídica. Actualmente, este proceso se le facilita mucho cuando existe una estructura social virtualizada la cual ofrece una gran fuente de información en el momento conocida como redes sociales.

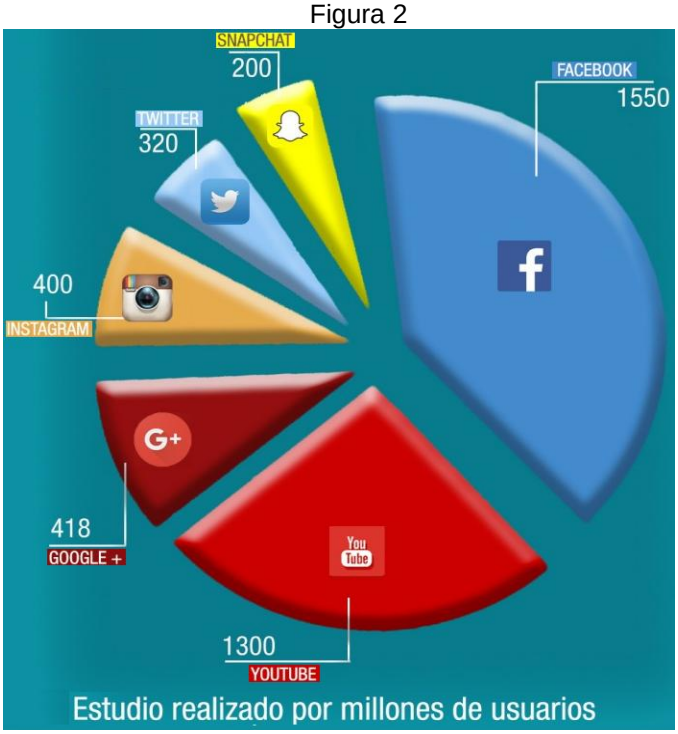
Puede parecer que las redes sociales son un servicio moderno, sin embargo, su historia puede remontarse a varias décadas atrás. Fue hacia la década de los 90 donde se inició el furor por las mismas y continua en la actualidad logrando una verdadera masificación de la mano de diferentes dispositivos móviles y la conectividad a internet marcando una nueva tendencia en la comunicación.

Actualmente existen gran cantidad de redes sociales como facebook, twitter, youtube, instagram, whatsapp, linkedin, google+, line, hi5, badoo, entre otras, donde se han convertido en una moda para algunos y en casos más drásticos en una total dependencia. Estos servicios abrieron unos escenarios didácticos, entretenidos y sencillos para la integración de todo tipo de personas y culturas facilitando la creación de grupos con ideas afines para apoyar diversas causas o simplemente por si alguien desea compartir un pensamiento, una foto, un video o algún dato, ya sea con sus amigos o familiares. Si se toma el tiempo de mirar de una manera objetiva la información que se publica sobre algunos perfiles, sin mayor esfuerzo se pueden obtener direcciones, teléfonos, conocidos, gustos, círculo social e información laboral, prácticamente una descripción detallada de la persona dueña de la cuenta y toda esta información puede ser aprovechada por alguna persona que tenga algún interés con fines delictivos.

Es una manera muy efectiva para poder perfilar posibles víctimas y clasificarlas ya sea porque son el objetivo o para usarlas como medio y llegar a personas específicas a través de la creación de confianza, engaños y astucia y poder incurrir en acciones como robo de credenciales, contraseñas, información financiera, etc.

Cuando el objetivo no es una persona en específico sino lo que se busca es encontrar víctimas potenciales, las redes sociales son una excelente oportunidad para ello. Actualmente cada una de las compañías que ofrecen el servicio de red social poseen entre cientos y millones de usuarios registrados y aún se siguen sumando más personas y de todos estos siempre se podrá encontrar alguno que no esté informado o preparado para detectar a un atacante y sus técnicas. A continuación se muestra una infografía con información del número de usuarios de las redes sociales más populares en el momento, ver figura 2.

Figura 2




*Redes sociales más usadas en el 2016*
*Fuente: http://www.multiplicalia.com/redes-sociales-mas-usadas-en-2016/*

Las redes sociales se presentan como una gran oportunidad para las personas malintencionadas ya que dan facilidad para el anonimato, para la creación de perfiles falsos y de esta manera engañar. Los objetivos pueden ir desde lo económico, por contratación, por gusto, para medir habilidades y técnicas, por competir, como un juego o simple entretención. Luego de seleccionar a la víctima y de evaluar la información del perfil que se encuentra publicado procede a generar la creación de un perfil falso, generalmente de sexo contrario, y poder establecer un primer contacto, en su mayoría con fines afectivos.

Una vez ganada la confianza del usuario, procede a compartir contenido con la víctima enviándole archivos de interés o remitiéndolo a sitios para infectar el equipo o dispositivo con software malicioso, keylogger, entre otros, y de esta manera acceder y capturar información para alcanzar su objetivo. Algunos atacantes van más allá de comprometer a una sola persona, aprovechando que lograron instalar software mal intencionado en los dispositivos de sus víctimas, roban las credenciales de acceso de sus respectivas redes sociales, correo y demás para poder usar este perfil y atacar de la misma forma a los contactos del usuario, comprometiendo más sistemas y así sucesivamente.

## IV. CONTRAMEDIDAS Y DEFENSAS

*"Usted puede tener la mejor tecnología, firewalls, sistemas de detección de ataques, dispositivos biométricos, etc. Lo único que se necesita es un llamado a un empleado desprevenido e ingresar sin más. Tienen todo en sus manos."*[4]

Las maneras de usar la ingeniería social para comprometer algún tipo de información ya sea de un individuo o de toda una organización cada día evolucionan más. Técnicas más audaces e imperceptibles que la convierten en un riesgo al cual hay que prestarle la debida atención, pero no solo los atacantes mejoran sus métodos, las personas que logran detectar este tipo de engaños pueden desarrollar contramedidas y en un ambiente corporativo la seguridad de la información se involucra de manera directa. Casos como el de David Kennedy, fundador y CEO de trustedsec y co-fundador y chief technology officer de binary defense systems (BDS) quien comenzó trustedsec con la visión de hacer mejor la industria de la seguridad de la información con el desarrollo de herramientas como SET (social-engineering tool kit).

SET: Es una completa suite dedicada a la ingeniería social que permite automatizar tareas como envío de sms (mensajes de texto) falsos con los que se puede suplantar el número telefónico que envía el mensaje, clonar páginas web y poner en marcha un servidor para hacer phishing, envío de archivos adjuntos a través de correos electrónicos para que al abrirlo ejecute software que puede permitir tomar control del equipo o capturar información. Está especialmente diseñado para realizar ataques

[4]Mitnick, K. (s.f.). Obtenido de https://societyandhacking.wordpress.com/fuente-3/

avanzados contra el elemento humano, por este motivo se ha convertido en una herramienta estándar en el arsenal de los pentesters ya que permite verificar el nivel de vulnerabilidad de una organización ante ataques de ingeniería social y poder tomar las medidas correspondientes.

Los sistemas de seguridad de la información deben integrar los procesos, la tecnología y las personas. Estas últimas serán tan vulnerables como su propio desconocimiento ante las técnicas citadas anteriormente, por ello la principal defensa contra la ingeniería social es el conocimiento. Un método efectivo por parte de las organizaciones es la capacitación, entrenamiento y promoción de buenas prácticas donde idealmente el usuario las adopte no solo como una medida organizacional, sino como un plus que le servirá para su propio entorno personal y familiar.

Las siguientes son algunas actividades que ayudan a mitigar los casos de ingeniería social, para aplicar a nivel corporativo o personal dependiendo el caso:

- ✓ Involucrar en las capacitaciones a la totalidad de los usuarios, desde los directivos hasta el personal de limpieza.
- ✓ Contar con políticas de seguridad que cubran aspectos de ingeniería social y realizar los controles respectivos para garantizar su entendimiento y cumplimiento.
- ✓ Desconfiar de correos con contenidos alarmantes no esperados, de fuentes poco habituales o cuyo contenido incite a la curiosidad, donde al dar click dirija a noticias relacionadas con actores, deportes, tragedias, eventos políticos, etc. En estos casos, siempre comprobar las fuentes y en caso de ser necesario el establecer algún contacto, remitirse a las fuentes oficiales y no a las que contiene el correo.
- ✓ Antes de abrir cualquier archivo adjunto o archivos contenidos en una usb, analizarlos con un antivirus actualizado.
- ✓ No ejecutar programas de procedencia desconocida.
- ✓ No arrojar documentación técnica ni sensible a la basura, ejecutar el procedimiento de destrucción adecuada.
- ✓ No revelar información personal por correo electrónico, ni en línea, a menos que se tenga la certeza de que es un procedimiento legítimo.
- ✓ Uso de contraseñas seguras evitando fechas de nacimiento, nombre propio, o información personal que sea fácilmente asociable.
- ✓ Evitar en lo posible redes para compartir archivos (peer-to-peer).
- ✓ Si por algún motivo a través de un correo, una llamada o cualquier procedimiento fuera de la cotidianidad incita a apartarse de las normas de la empresa, lo ideal es reportar y seguir al pie de la letra los procedimientos instaurados.

Para el caso de las redes sociales tener en cuenta:

- ✓ Controlar muy bien las restricciones de quienes tiene derecho a visualizar la información y evitar que se exponga de manera pública.
- ✓ No aceptar cualquier solicitud de amistad.
- ✓ No descargar archivos que procedan de sitios sugeridos por desconocidos o que parezcan sospechosos de alguna manera.
- ✓ Desconfiar, o prestar la atención necesaria a la amistad que ha escalado de manera precipitada.
- ✓ Si de alguna manera se detecta que uno fue objeto de un ataque, notificar a los conocidos para que tomen medidas de precaución como actualización de contraseñas y escaneo de sus equipos.

## V. CONCLUSIONES

El ser humano siempre está en la búsqueda de información ya sea de su ambiente o de las personas que lo rodean, con el objetivo de poder utilizarla para lograr algún tipo de beneficio valiéndose de cualquier medio para ello. Este actuar puede darse de una manera natural y se vuelve más complejo y especializado con el paso del tiempo y con la interacción social, y es cuando ya sea consciente o inconscientemente se desarrollan técnicas específicas que para algunos es simple rutina que lleva a un fin pero para otros que le prestan más atención y lo desarrollan a otro nivel lo llaman ingeniería social. Estas técnicas tienen como fin aprovecharse de la ingenuidad, desconocimiento y la confianza de las personas para hacerlos realizar actividades que normalmente no harían, confianza que ganan a través de la persuasión ya que el secreto no está en preguntar sino en la forma de realizar la pregunta. En la actualidad pocos tienen conocimiento de estas técnicas y el impacto que pueden llegar a tener tanto a nivel de un individuo como a nivel de una organización y algunos otros no le brindan la suficiente importancia ya que consideran que a ellos nunca les va a suceder, por motivos como estos actualmente para los atacantes el uso de la ingeniería social se convirtió en una herramienta demasiado efectiva, si se desea atacar a una persona o a una organización para robar datos financieros, contraseñas de acceso o información sensible la debilidad humana es mucho más fácil de penetrar que las debilidades de la red.

El uso de la ingeniería social va más allá de los conocimientos técnicos, involucra el desarrollo de habilidades sociales, técnicas psicológicas y toda una preparación para buscar vulnerabilidades en las personas levantando tanta información como sea posible de los mismos y en el momento esta información también puede conseguirse de una manera rápida y eficiente gracias a las redes sociales, permitiendo adquirir información que ayuda a planear un engaño con mucha más eficiencia y en total anonimato. Por más que sea una técnica tan usada y eficiente, no implica que no se pueda tener una defensa contra la misma y la manera de enfrentarla comienza con el conocimiento y la generación de conciencia, hacer lo posible para estar al tanto y aplicar las recomendaciones que ofrecen las entidades de confianza y las respectivas organizaciones sobre el uso de los sistemas. Recomendaciones como la instauración de contraseñas seguras, desconfiar de información no esperada, ante correos o mensajes intimidantes sobre asuntos personales y no remitirse a la información que viene adjunta, sino contactar directamente al ente que supuestamente la genera o como algunos autores sugieren, desconfiar de todo hasta un punto de paranoia aceptable, donde tenga la certeza que la información que me brindan es completamente verídica.

## REFERENCIAS


[1] Borghello, C. (13 de Abril de 2009). *El arma infalible: la Ingeniería Social*. Obtenido de http://www.eset-la.com/pdf/prensa/informe/arma_infalible_ingenieria_social.pdf

[2] *Fraude en línea: pharming*. (s.f.). Obtenido de http://www.symantec.com/region/mx/avcenter/cybercrime/pharming.html

[3] Granger, S. (03 de 11 de 2010). *Social Engineering Fundamentals, Part I: Hacker Tactics*. Obtenido de http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics

[4] Micro, T. (2012). *5 motivos por los que las trampas*. Obtenido de http://www.trendmicro.es/media/br/5-reasons-why-social-engineering-tricks-work-es.pdf

[5] Mitnick, K. (s.f.). Obtenido de http://www.pandasecurity.com/spain/mediacenter/seguridad/ingenieria-social-empresas/

[6] Mitnick, K. (s.f.). Obtenido de http://www.securityfocus.com/news/199

[7] Mitnick, K. (s.f.). Obtenido de https://societyandhacking.wordpress.com/fuente-3/

[8] Mitnick, K. (30 de 04 de 2001). *My first RSA Conference*. Obtenido de http://www.securityfocus.com/news/199

[9] Toffler, A. (s.f.). Obtenido de http://jackelinemedinaarbi.blogspot.com.co/2011/02/reflexiones-sobre-la-tercera-ola-de.html