

Ingeniería Social

Autor: Daniel Antokoletz Huerta

Edición y Corrección: Lic. Cristian Borghello, MVP - CISSP

Fecha Publicación: 25 de mayo de 2010

Publicado en [Segu-Info](http://www.segu-info.com.ar)

Daniel Antokoletz es el Responsable IT de Intraway Corp. Durante 20 años fue el responsable IT de SADAIC, ha sido docente en la UTN-FRBA y ha trabajado en investigación de inteligencia artificial y algoritmos genéticos.

*Todo el Arte de la Guerra se basa en el engaño.
El supremo Arte de la Guerra es someter al enemigo sin luchar.*

Sun Tsu, El arte de la guerra.

Índice

Ingeniería Social	1
Índice	2
1.- Introducción	3
2.- Definiciones	5
3.- La ingeniería social y las ciencias del comportamiento	7
3.1.- Teorías de la motivación.....	7
3.2.- Comportamiento de grupo	8
3.3.- Liderazgo.	9
3.4.- Cultura.....	9
3.5.- Comunicaciones.....	10
3.6.- El cambio organizacional.....	11
3.7.- Poder e influencia.	11
4.- Bases de la ingeniería social	12
4.1.- ¿Cuáles son los elementos que nos hacen tan permeables al uso de la Ingeniería social? Principios de persuasión	12
4.2.- La sociedad, gran inculcadora de permeabilidad a la ingeniería social.	14
5.- Anatomía de un ataque de ingeniería social	17
5.1.- Conocimiento del blanco.	17
5.2.- Los rasgos de un rol.	18
5.3.- Lograr credibilidad.	19
5.4.- Lograr que el blanco asuma un rol.	20
5.5.- Desviar la atención del pensamiento sistémico.	20
5.6.- Explotar el impulso de la conformidad.....	21
5.7.- El deseo de ayudar.	22
5.8.- Ganarse la simpatía del blanco.	22
5.9.- Explotar el miedo.....	23
5.10.- Explotar la reactancia.....	23
6.- Un par de ejemplos prácticos e históricos	25
6.1.- El génesis y un mito egipcio	25
6.2.- Entrada al partido de futbol.	27
6.3.- El vecino molesto.....	29
6.4.- Test de penetración.	31
6.5.- Blanco en el Foro.....	35
7.- Cómo protegerse de un ataque de ingeniería social	39
Glosario	41
Referencias	43

1.- Introducción

En el ambiente de la seguridad, se busca tener en cuenta a todas las posibles amenazas que acechan a la información y a los datos. Una de esas posibles amenazas son los ataques de ingeniería social, los cuales son tan importantes que la mayoría de los libros y certificaciones tienen dominios exclusivos para su estudio.

En el artículo Ingeniería social y psicología publicado ^[AF01] en El País, Alfredo Fierro, nos adelanta que *“El propósito de transformar al hombre es tan antiguo como el hombre mismo. Ha sido un propósito ya descaradamente interesado - influir en el otro, individualizado o colectivo, para aproximarlo a nuestra conveniencia-, ya desinteresado, al menos en la apariencia de la intención: aliviar sus males, mejorarlo, modificar su vida para su propio bien”*. ¿Quién decide qué es lo bueno o lo malo para las personas? Ese es otro problema. Aquí nos enfocaremos en algunas técnicas que se usan para conseguir que las personas cumplan nuestros deseos.

Desde el momento que vivimos dentro de una sociedad, estamos expuestos a ciertos tipos de manipulación que no siempre es por nuestro propio bien o por el bien común, pero que en todos los casos nos puede dejar enseñanzas.

Analicemos los siguientes ejemplos sencillos. ¿Qué pueden tener en común los casos enunciados?

Veamos las siguientes situaciones:

“Un niño se encuentra frente a un plato de comida que no tiene intenciones de comer. La madre del niño, distrae su atención con cantos y juegos mientras, cuchara a cuchara, vacía el plato en la boca del niño quién lo engulle sin darse cuenta”.

“Un niño, por la noche, despliega todo su encanto y llena a su padre de elogios y le cuenta las cosas que hizo durante el día para poder conseguir que lo dejen jugar un rato más antes de dormir”.

“En la salida del subte, un mendigo que no es ciego, se sienta en el piso simulando serlo, con unos anteojos oscuros y un palo pintado de blanco mientras sacude un jarrito con un par de monedas, invitando a los transeúntes a que le den limosna aprovechando el sentimiento de lástima”.

“En cualquier canal de televisión podemos vernos bombardeados por comerciales que utilizando técnicas que veremos en el presente documento, crean la necesidad de compra de algunos productos”.

“Un político, en plena campaña y previo a un discurso, analiza al grupo a quién irá dirigido el mismo para endulzar sus oídos o provocarles temor de lo que podría suceder si gana el otro partido político”.

“El gobierno de un estado explota una catástrofe natural o artificial para desviar la atención de la población de problemas más profundos. En el ambiente político se lo denomina cortina de humo (un buen ejemplo de ésto es el uso de la quema descontrolada de pastizales que afectaron a la Ciudad de Buenos Aires, Rosario, Campana, etc. para descomprimir la atención del problema rural y de la inflación).”

Si bien en el primer caso, la actuación de la madre es muy bien intencionada; la actuación del hijo, en el segundo caso, es totalmente inocente; puede lindar en el delito como es el caso del estafador que se hace pasar por ciego en el tercer caso; o tiene fines comerciales o promocionales como es el caso de las propagandas o en el caso del político; todos los casos tienen algo en común.

Ese algo son las técnicas que utilizan en cada uno de los casos. Todas esas técnicas, entran dentro de las que se usan en la ingeniería social.

De hecho, en cada caso y a su manera, se está haciendo ingeniería social.

Como puede entreverse en ésta introducción, en el presente trabajo, nos enfocaremos en la ingeniería social como arma contra la sociedad organizada, como abuso del sistema contra el sistema.

NOTAS:

En el presente trabajo se relatan acciones que, la mayoría, van reñidas con las buenas costumbres y, algunas desde hace muy poco tiempo, por una modificación en el Código Penal de la República Argentina, constituyen delito en el territorio argentino, otra, siempre fueron ilegales..

Los relatos de incursiones y los casos prácticos fueron obtenidos de distintos foros hacker, y son publicados en el presente trabajo con permiso de los perpetradores que se dan a conocer por “nicks” o pseudónimos. El autor no tiene manera de corroborar la exactitud de los de los relatos, como tampoco la identidad de los perpetradores pero sirven para fines educativos. La excepción son algunos relatos que me sucedieron en el ámbito laboral que pude comprobarlos personalmente. Todos los casos se mencionan con el fin de que pueda comprenderse el modus operandi de los ingenieros sociales y crackers con el fin de poder prepararse y evitar caer en sus redes, evitando de este modo incurrir en posibles conductas delictivas. Los crackers, en muchos casos tratan de lograr que el blanco/víctima se convierta en sus cómplices.

2.- Definiciones

Son muchas las definiciones que pueden darse de ingeniería social. Analicemos algunas de ellas:

En la wikipedia (que es la enciclopedia libre) podemos encontrar que la definición de ingeniería social se aplica a dos grandes áreas a las ciencias políticas^[W101] y a la seguridad informática^[W102].

En la primera acepción podemos ver que *“es un concepto de las ciencias políticas que se refiere a los esfuerzos para influir las actitudes populares y el comportamiento social a gran escala, sea por los gobiernos o por grupos privados.”*

Por otra parte en su segunda acepción, con respecto a la seguridad informática, *“es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos”*.

Sara Granger en su página Social Engineering Fundamentals, Part I: Hacker Tactics, define a la ingeniería social como *“el arte y la ciencia de hacer que la gente cumpla con tus deseos”*^[SG01].

Viendo estas definiciones y muchas otras que pululan por internet, podemos delinear la siguiente definición:

La ingeniería social es el empleo de técnicas y acciones premeditadas que permitan manipular las acciones de las personas para lograr que realicen tareas que, naturalmente, no harían.

Por medio de la ingeniería social, no sólo es posible conseguir acceso a información confidencial de una empresa y quizás el control de sus servidores y redes sino que se puede afectar significativamente la vida de cualquier internauta. Todos conocemos lo molestos que son los SPAM o correos basura en donde nos ofrecen las más variadas cosas y muchas veces contaminan las máquinas de los internautas con virus, troyanos, keyloggers y spyware^[MA01]. En realidad éstas molestias son productos de la ingeniería social.

¿Cuántas veces recibimos cadenas donde dice que por cada email que enviemos, depositarán un centavo en la cuenta de una niña que necesita una operación de una enfermedad terrible (o algo similar)? ¿Cuántas de esas veces nos sentimos apesadumbrados por la mala suerte de esa infanta y reenviamos el correo a toda nuestra lista de contactos?

Otras veces recibimos cadenas de la amistad, y como no queremos ser odiosos y queremos tener muchos amigos, tomamos toda nuestra lista de contactos y la hacemos destinataria de nuestra amistad.

Todas éstas son algunas de las técnicas que utilizan los ingenieros sociales para obtener enormes bases de datos de correos electrónicos para vender a las

empresas que realizan promociones por Internet (lo que comúnmente se conoce como SPAM o Correo basura).

La ingeniería social se basa en la confianza. El ingeniero social busca que la víctima confíe plenamente en él o por lo menos lo suficiente para que no sospeche que será timada.

Uno de los objetivos principales de la ingeniería social en el ámbito organizacional es obtener acceso a sistemas de información de manera clandestina. Los motivos de esa búsqueda de acceso puede abarcar desde simple curiosidad y “autotestearse” (ver hasta dónde puedo llegar sólo por la emoción de lograrlo; muchos testimonios de perpetradores coinciden en que el flujo de adrenalina que provoca el realizar esas intrusiones son comparables a escalar grandes montañas; coinciden en que el sentimiento de logro es el mismo), hasta cometer fraudes y realizar espionaje industrial.

Como veremos más adelante, en la seguridad organizacional, el punto más flaco es, sin duda las personas. Es muy difícil luchar contra la ingeniería social.

El mítico Kevin Mitnick^[KM01] ^[KM02] (uno de los hackers más famosos, convicto por penetrar en sistemas del gobierno Norteamericano y en varias empresas multinacionales, ahora reconvertido en consultor de seguridad) considera que más allá de las técnicas de hardware y software que se pueden implementar en las redes y en los servidores, el factor determinante de la seguridad de las mismas es la capacidad de los usuarios de interpretar correctamente las políticas de seguridad y hacerlas cumplir.

3.- La ingeniería social y las ciencias del comportamiento

Las ciencias del comportamiento, como todas las ciencias es amoral. Como cualquier herramienta, es el usuario el que decide el uso que le va a dar. Puede utilizarse para bien, para mejorar una organización, hacerla más eficiente y lograr que sea más agradable para los empleados; o puede utilizarse para manipular a la gente, para hacer que hagan cosas en beneficio de sólo uso pocos, incluso para manipularlas para que realicen acciones en contra de los intereses de la organización en la que están insertos.

Realizaremos un pantallazo de algunos puntos generales que estudian las ciencias del comportamiento y trataremos de determinar cómo se beneficiaría el ingeniero social y cómo aprovecharía esa herramienta en contra del sistema.

Abarcar todos los estudios de las ciencias del comportamiento sería imposible, de manera que veremos sólo la aplicación de algunos tópicos:

3.1.- Teorías de la motivación

Una de las principales herramientas a la que echa mano un ingeniero social, son las teorías de la motivación.

En el análisis previo que el atacante realiza de la empresa, intenta de determinar, entre otras cosas las estrategias de motivación y conducción.

Las ciencias del comportamiento buscan respuestas a preguntas como ¿Por qué trabajan las personas? ¿Qué necesidades se pueden satisfacer a través del trabajo? ¿Cómo se debe dirigir a las personas?

Algunas respuestas a estos interrogantes la ofrecen los supuestos o creencias. Estos supuestos provienen de los supuestos básicos subyacentes (el cual busca como motivar correctamente a las personas).

Normalmente, se estudian cuatro supuestos que tienen aplicación desde diferentes momentos de la historia. Enfatizo la palabra desde porque, en la actualidad, todavía hay organizaciones que basan su motivación en los primeros supuestos.

- Racionales-económicos: (1880) Según estos supuestos, la motivación de los empleados es de índole material, los administradores piensan que los empleados hacen cualquier cosa que les asegure mayor ganancia de tipo económico. El empleado es considerado un agente pasivo a quien la organización debe manipular, motivar y controlar. Deben mantenerse bajo control a los sentimientos.
- Sociales: (1930) Según estos supuestos, consideran que el principal motivador, son las necesidades sociales y las relaciones interpersonales

son las que dan origen al sentido de identidad. Los empleados responderían más ahora a las fuerzas sociales de los grupos, que a los incentivos y controles de la empresa.

- Actualización: Para los administradores seguidores de éste supuesto, la motivación de los empleados tiene que ver con la necesidad inherente a los seres humanos de usar sus habilidades, autoafirmarse de modo creativo, autónomo, consciente y capaz de tomar decisiones. Las personas, en general, pueden motivarse y controlarse por si mismas.
- Complejos: (1970) Estos supuestos parten de considerar que el ser humano es un individuo mucho más complejo que el que se halla implicado en los diversos conceptos de hombre en los que se basan el resto de los supuestos. Se pueden aplicar cualquiera de los supuestos anteriores dependiendo del grupo humano y de la circunstancia.

Un ingeniero social analizaría la empresa y trataría de determinar qué supuestos son los preponderantes, y en base a ellos tratar de armar su estrategia de ataque: Obviamente si el atacante se encuentra ante una empresa que aplica preponderantemente los supuestos racionales económicos, el ingeniero social intentaría técnicas de acercamiento tentado al posible blanco con mejorar sus ingresos si le hace caso, o amenazándolo con posibilidades de perder económicamente. Aplicaría los principios de reciprocidad y de escasez.

Si se encuentra ante una preponderancia de lo social, buscaría aplicar el principio de aceptación social.

Si se encuentra ante una organización en dónde los empleados responde más a los supuestos de autoactualización, el ingeniero social intentaría aplicar el principio de escasez y el de reciprocidad, tentándolo con mayores conocimientos. Ante una sociedad que se base en supuestos complejos, deberá ir variando los principios o buscando el blanco más débil en alguno de los supuestos anteriores.

3.2.- Comportamiento de grupo

Sin duda, los ingenieros sociales se aprovechan sin lugar a dudas de los problemas de la interacción de las personas en los grupos y de los grupos entre sí. Los atacantes aprovecharán las debilidades que se presentan cuando los grupos se hallan en los primeros estadios de su formación en la primera etapa o de formación y en la segunda (la llamada de conflicto) cuando hay gran incertidumbre ante la finalidad, estructura y liderazgo del grupo. Los integrantes ofrecen resistencia a abandonar su individualidad.

Sin duda en los siguientes estadios, el ingeniero social buscará a los miembros más débiles o, quizás a algunos que hayan quedado resentidos luego de la asignación de roles y estatus.

Cuando el grupo es informal, los pedidos y las recomendaciones pasan de boca en boca. El ingeniero social simplemente mencionará alguien de ese grupo

informal dotado de autoridad, y las puertas comenzarán a abrirse. Por otra parte, es muy difícil y requiere mucho análisis lograr formarse un “organigrama” de la estructura informal. En el caso de los grupos formales, podrá fingir un rol, es posible que tenga que luchar contra algo de burocracia, pero es más sencillo de preparar ya que los roles están delimitados y plasmados físicamente. Y con simples preguntas uno puede hacerse una idea de cuál es la cadena de mando. Como veremos más adelante, los ingenieros sociales pueden aprovechar su capacidad para representar diferentes roles de integrantes del grupo.

3.3.- Liderazgo.

Las ciencias del comportamiento han estudiado mucho el tema del liderazgo. Se sabe que el liderazgo es una interacción entre tres factores: el líder, los colaboradores y las circunstancias. Los ingenieros sociales, deben entrenarse como líderes, teniendo en cuenta que, a diferencia de los líderes de las organizaciones, debe considerar como su colaborador al blanco o a los blancos seleccionados.

Una vez que un blanco aceptó el liderazgo de un ingeniero social habilidoso, es extremadamente difícil poder recobrar su independencia ya que el blanco se verá cada vez más enredado y por ende cada vez más dependiente del ingeniero social.

3.4.- Cultura.

Como veremos más adelante, en la anatomía de un ataque de ingeniería social, lo primero que realizará el perpetrador, es realizar un estudio, lo más exhaustivo posible de la realidad de la organización a donde dirigirá su ataque.

El psicoanalista inglés Eliot Jaques define a la cultura en una organización como *“la manera acostumbrada y tradicional de pensar y de hacer las cosas que está compartida, en mayor o menor medida por todos los miembros y que los nuevos miembros deben aprender y, por lo menos parcialmente, acatar para ser aceptado cuando entren a prestar servicios en la firma.*

La cultura en ese sentido cubre un amplio ramo de conductas:

- *Métodos de producción*
- *Pericias ligadas a tareas específicas y conocimientos técnicos*
- *Actitudes relacionadas con la disciplina y los castigos.*
- *Las costumbres y hábitos de la conducta administrativa.*
- *Objetivos de la empresa*
- *La manera de hacer negocios de la empresa.*
- *Los métodos de pago*
- *Los valores asignados a los distintos tipos de trabajo*
- *Las creencias en la vida democrática y en la concertación*

- *Los tabúes menos conscientes*

La cultura es parte de una segunda naturaleza para aquellos que han estado en la firma durante algún tiempo. La ignorancia de la cultura caracteriza a los novatos mientras que los inadaptados son los que rechazan la cultura...”

Uno de los puntos fundamentales es determinar la cultura de la organización. La definición que he seleccionado de cultura, ya de por sí deja bien en claro cuáles son las bondades que tiene el conocimiento de ésta para un ingeniero social: poder determinar cuál será el comportamiento del blanco en diferentes circunstancias, cuáles son los límites entre los que debe moverse el ingeniero social y cómo moverse (con esto quiero decir qué gestos son comunes dentro de la organización y que deberá imitar, cual es el lenguaje apropiado; si tiene que presentarse en persona, cuál es la vestimenta conveniente, que jerga utilizan, etc.).

De los puntos enunciados en la definición, hay tres que, su conocimiento proporciona a los ingenieros sociales una ventaja invaluable: Actitudes relacionadas con la disciplina y los castigos; las costumbres y hábitos de la conducta administrativa y los tabúes menos conscientes.

3.5.- Comunicaciones.

Uno de los procesos organizacionales que estudian las ciencias del comportamiento son las comunicaciones dentro de una organización. Es un proceso omnipresente en toda interacción humana.

La comunicación consiste en la transferencia de información y comprensión de la misma entre dos personas, dos grupos o dos sistemas de la organización.

En la comunicación intervienen distintos factores, que el ingeniero social sin duda explotará:

1. Lugares donde se realiza la comunicación
2. distancia física entre los interlocutores
3. Soporte utilizado
4. Status de los interlocutores
5. Experiencias previas
6. Personalidad de los interlocutores
7. Motivaciones para comunicarse
8. Conocimiento de los hechos o situaciones que han generado la comunicación
9. La elección del código o las palabras por parte de los interlocutores.
10. Manera de expresarse, el ritmo, la entonación del discurso (tanto oral como escrito).
11. El lenguaje no verbal: gestos, expresiones, miradas, etc.

El ingeniero social se vale casi exclusivamente de las comunicaciones para realizar su ataque, de manera que presta muchísima atención al uso de los factores mencionados.

3.6.- El cambio organizacional.

En la época actual, las organizaciones se encuentran en constante cambio y esto hace que los miembros de la organización tengan que estar en un período de adaptación constante. Cambios en la economía global, globalización, fusiones, escisiones, mejoras tecnológicas, descubrimientos, regulaciones... Son muchísimos los factores que obligan a las organizaciones a mantenerse en esa ola de cambios. Esta constante inestabilidad, da al ingeniero social, un terreno en el que moverse donde puede afianzarse fácilmente.

Veamos la experiencia que nos relata johnconnor, de un ataque que perpetró hace un par de años:

“Hace tiempo que buscaba colarme en esa empresa. Siempre me dijeron que era imposible... para mí no existe lo imposible. Investigando por Internet, descubrí que la empresa había sido comprada por un grupo empresario. Llamé a la telefonista y luego de hablar un rato con ella, decirle que tenía que hacer una maldita encuesta por el tema de la adquisición, no solo escuché un movimeito de inquietud, sino que luego, la mujer hablaba más tensa. Sin presionar mucho obtuve una lista de nombres e internos bastante atractiva. Llamé a desarrollo y con el mismo rollo de la encuesta por la adquisición, logré obtener las llaves del reino: un par usuario-contraseña totalmente activos...”

3.7.- Poder e influencia.

Dado que el poder y la influencia son procesos organizacionales de una importancia superlativa a la hora de realizar una incursión de ingeniería social, los estudiaremos con detenimiento en las bases de la ingeniería social.

4.- Bases de la ingeniería social

Como expresamos en el punto anterior, los basamentos principales de la ingeniería social son las ciencias del comportamiento. Como dijimos el tema del poder y la influencia tienen una gran importancia al momento de realizar un ataque, de manera que en éste punto me explayaré sobre los mismos.

Las ciencias del comportamiento distinguen las cinco bases del poder:

- Autoridad
- Capacidad de aplicar castigos
- Capacidad de aplicar premios
- Experto
- Carisma

Las dos últimas son aptitudes personales, entrenadas o aprendidas.

El ingeniero social se entrena para adquirir las dos últimas bases del poder y, además, para poder simular tener las otras.

4.1.- ¿Cuáles son los elementos que nos hacen tan permeables al uso de la Ingeniería social? Principios de persuasión

Según Cialdini, Wissler y Schweitzer^[CWS01] hay seis principios de la persuasión. Son las maneras en las cuales algunas personas pueden influenciar y persuadir aprovechando las debilidades fomentadas por la cultura de la sociedad en la que vivimos.

- *Principio de agradabilidad:* La gente puede ser influenciada mucho más fácilmente por las personas que le agradan. Cuando las personas sienten similitud por otras tienden a ser influenciadas por ellos. Son muchas las maneras que una persona puede agradar a otra: atracción física, intereses comunes, sufrimientos comunes, similitud de fines, etc.
Una aplicación muy común es una de las técnicas que utilizan algunos adolescentes varones, para conquistar a las chicas. Lo primero que hacen es buscar (o inventar) puntos en común. Tener gustos similares, aplicar la atracción física, si la hay; entrar en los mismos grupos de interés, etc.
Este mismo principio se puede utilizar muy fácilmente cuando se necesita que cierta persona ejecute algún troyano, algún keylogger o algún virus.
- *Principio de autoridad:* Las personas son más fácilmente influenciadas por aquellas en las que perciben cierta autoridad (legítima o no).

En muchas ocasiones, el hablar o comportarse con cierta autoridad, abre muchísimas puertas.

De acuerdo a las bases del poder estudiadas por las ciencias del comportamiento (Autoridad, Capacidad de premiación, capacidad de castigo, poder experto y carisma) si una persona percibe en otra algún tipo de poder, tendrá tendencia a ser influenciada por ella.

Cuanto más estructurada y jerárquica sea la organización, mayor será la facilidad con que los estamentos inferiores puedan ser influenciados. Un caso muy especial son los cuerpos militares o de seguridad. Si los estamentos inferiores no están perfectamente entrenados en exigir pruebas de autoridad (credenciales, atributos, jinetas, etc.), son fácilmente influenciados y dominables por cualquiera que sepa ejercer el poder y que conozca la jerga correspondiente. Ver casos prácticos.

- *Principio de escasez:* Las cosas y oportunidades son cada vez más deseables cuando ellos sean menos accesibles. Un caso típico de este principio, es el hecho que está sucediendo estos días en ocasión de la protesta de los ruralistas apoyada por los propietarios de los transportes en contra de las retenciones del gobierno. Bastó que un periodista mencionara que, debido al paro y la protesta, faltarían alimentos, para que los supermercados fuesen depredados, acelerando el proceso de desabastecimiento que, teniendo en cuenta la modalidad de la protesta, nunca debería suceder.

Un caso típico de aplicación de este principio en el ámbito organizacional es el caso del atacante que se pone en contacto con un usuario diciéndole que tendrá problemas con su computadora y que, por cierta cantidad de tiempo, no podrá usarla (genera la escasez) y para evitar esa escasez, debe ejecutar tal o cual programa, activando un antivirus, un keylogger, o un troyano.

- *Principio de consistencia:* Toda persona tiene un fuerte deseo de ser consistente con sus opiniones, aseveraciones y acciones previas. Muchos atacantes que usan ingeniería social, buscan que un empleado responda preguntas manejándolas como preguntas inocentes, y mechar entre ellas una pregunta comprometedoras. Si se le hiciera directamente la pregunta comprometedoras, el empleado seguramente no la respondería, pero insertada dentro de varias preguntas “inocentes”, ya que comenzó a colaborar respondiendo esas preguntas, será consistente respondiendo la misma pregunta comprometedoras.

- *Principio de reciprocidad:* La gente tiene tendencia a devolver los favores. Cuando una persona recibe algo, tiene tendencia a quedar en deuda con la quién que se lo da y, de cierta forma, el receptor tiene tendencia a ser influenciado por el dador.

Un experimento muy sencillo que puede realizarse es entrar en una oficina y sonreírle a la gente. Más del ochenta por ciento de los empleados que reciban ese trato, responderán del mismo modo.

En las organizaciones es uno de los principios más peligrosos. Porque el terrible dicho favores con favores se paga puede terminar publicando el secreto más caro de la empresa. Ver en los casos prácticos una aplicación muy clara de éste principio.

- *Principio de la aceptación social:* Muchas personas deciden hacer lo que ven que hacen personas similares a ella.

Esa pregunta que se realiza a las personas que hacen todo lo que otra persona hace “*Si fulanito se tira debajo de un tren, vos también lo hacés*” hace referencia al principio de aceptación social.

Es muy fácil ver éste principio en cómo la gente sigue las modas, o se inserta en un frenesí consumista para poder estar igual que los demás, para ser aceptado por los demás.

Una de las observaciones que realiza un ingeniero social para intentar aplicar éste principio a una persona, es verificar si cómo va vestido, qué atuendos utiliza. Si el blanco viste a la moda, está muy bien arreglado, demuestra interés sobre lo que los demás piensan de él, es un fieme candidato para que parte del ataque de ingeniería social se base en éste principio.

4.2.- La sociedad, gran inculcadora de permeabilidad a la ingeniería social.

Desde que somos niños, se nos va preparando lenta pero inexorablemente, para insertarnos en una sociedad que tiene valores muy hermosos pero, mal aplicados, muy peligrosos.

Cuando somos niños, nuestros padres, con la mejor intención y buscando nuestra felicidad, nos van guiando para que nuestro comportamiento sea acorde a lo se espera y evitar el rechazo de los demás.

Debo aclarar que es un tema muy complicado y delicado ya que en buena medida es bueno: hace que no nos matemos entre nosotros y que nos preocupemos mínimamente por el prójimo. Pero como toda herramienta, sobreaplicarla provoca una masificación de los seres humanos rayana en el fanatismo.

Veamos los siguientes casos que suceden a una edad muy temprana:

- Si no desayunas bien, tu amiguito te va a ganar en todas las carreras y nadie va a querer estar cerca tuyo (competitividad y aceptación).
- A todos los niños le gusta el football, mejor que aprendas un poco porque si no te vas a quedar fuera del grupo.
- Si no saludas, te vas a quedar solo.
- Como todos los niños miran tal o cual programa de televisión, le ponemos el mismo programa para que tenga algún tema de conversación, así no se queda solo (se va generando una obligación pasiva a través de las repeticiones).
- En muchas escuelas, a fin de poder manejar bien a los niños, le implantan pautas de comportamiento, utilizando la aceptación o rechazo del grupo, como ponerlos en evidencia, ridiculización, etc.
- Si no ordenas, te tiro los juguetes (realización por miedo al castigo).
- No vas a salir a jugar afuera porque yo te lo digo (aplicación de la autoridad sin razonamientos).

A medida que los niños van creciendo, muchos de estos comportamientos aprendidos son la base de las conductas y de las personalidades que luego definirán al adulto y que lo pondrán en situación de ser víctimas de ingeniería social aplicada por atacantes sin escrúpulos, por empresas y por gobiernos.

Podríamos simplificar una clasificación de las personas utilizando dos animales:

- **Ovejas**
Las personas que forman parte de éste grupos, tienen una fuerte necesidad de aceptación grupal, están acostumbrados a los sistemas de premios y castigos como medios de incentivación. No tienen pensamiento individual, y si lo tienen, lo callan y adoptan inmediatamente el pensamiento de la mayoría. Tienen una gran tendencia al conformismo. Son blancos fáciles para la acción de ingenieros sociales.
Debo aclarar que el término ovejas no se aplica porque sean buenos o dóciles. Pueden ser extremadamente violentos.
Son personas que se manejan como masa. Como veremos más adelante, en éste grupo el pensamiento predominante es heurístico.
En la realidad que nos toca vivir (año 2008), las personas de bajos recursos conocidas como piqueteros, son un ejemplo típico de ésta clasificación.
- **Lobos**
Los lobos, son personas que pueden llegar a reunirse en grupo, pero no son grupodependiente. Tienen, por lo general, personalidades fuertes y se manejan según sus convicciones. Por lo general fueron educados

racionalmente (con esto quiero decir que las reglas que debieron seguir le fueron claramente explicadas y se les ha enseñado desde pequeños a elegir y decidir). El pensamiento predominante en éste grupo es el sistemático. Las personas que conforman ésta clasificación, no son fácilmente manejables dada su costumbre de racionalizar. Por lo general, los ingenieros sociales pertenecen a éste grupo. Es muy difícil que un ingeniero social seleccione a una persona de éste grupo como blanco de ataque.

5.- Anatomía de un ataque de ingeniería social

Basándome en la descripción que realiza el Dr. Sagarín sobre los principios psicológicos en el libro “El arte de la intrusión” de Kevin Mitnik^[KM02], podemos establecer que hay una base común en el modus operandi de los ingenieros sociales:

5.1.- Conocimiento del blanco.

Los crackers y los ingenieros sociales llaman a esta etapa: *seguir el rastro*. Es la etapa en la que se busca tener un perfil completo de la manera de operar de la empresa objetivo.

Los objetivos de ésta etapa inicial incluyen determinar el ámbito en el que se desempeña la empresa blanco: sus actividades, sus conexiones, el ámbito geográfico en el que operan, si tienen sucursales, si tienen subsidiarias, las compañías o entidades con las que están relacionadas, fusiones o adquisiciones, nombres de contactos, correos electrónicos, números telefónicos, jerga, etc.

Cuanta más información reúna el atacante sobre el blanco, más efectivo será al momento de establecer su credibilidad con la víctima seleccionada (ver casos prácticos).

Este punto es una estrategia básica que se utiliza en todo tipo de ataques. Ya en la China antigua, época del maestro Sun Tzu, en su tratado “El arte de la guerra”^[ST01] podemos notar la importancia de recabar información sobre el enemigo como primer paso a un enfrentamiento exitoso: “*Si conoces a los demás y te conoces a ti mismo, ni en cien batallas correrás peligro; si no conoces a los demás, pero te conoces a ti mismo, perderás una batalla y ganarás otra; si no conoces a los demás ni te conoces a ti mismo, correrás peligro en cada batalla.*”

Esto lo corrobora otra cita de Sun Tzu: “*Siempre que quieras atacar a un ejército, asediar una ciudad o atacar a una persona, has de conocer previamente la identidad de los generales que la defienden, de sus aliados, sus visitantes, sus centinelas y de sus criados; así pues, haz que tus espías averigüen todo sobre ellos.*”

Los datos sobre la empresa blanco, pueden obtenerse de muchas fuentes; pero Internet es la más formidables de las fuentes.

Las Empresas son bastante descuidadas de la cantidad de información que proporcionan en las páginas web institucionales. Nombres, direcciones de correo electrónico, sucursales, números de teléfono, proyectos en los que están inmersos, etc.

Los buscadores como Google y Yahoo son herramientas poderosas en manos de los ingenieros sociales ya que pueden rastrear enormes cantidades de información sobre una empresa. Información trivial o molesta para un internauta común y corriente, pero información invaluable para un ingeniero social o un cracker. Con

respecto a los buscadores, transcribo un párrafo que me mandó KnOwSeEk a través de un foro hacker^{[HA01][HA02]}: *“No tienes idea de lo simple que es reunir información utilizando Google. Una vez tratábamos de entrar en la empresa AAA (Cambio el nombre para proteger a la víctima) y, mientras seguíamos el rastro, nos encontramos con un mensaje en un foro en dónde el administrador de la red de la empresa preguntaba cómo podía hacer para cambiar la contraseña por omisión del router Cisco modelo XXXX. No podíamos creer que el mismo administrador de red nos hiciera un regalo así. En menos de tres minutos estábamos dentro del router y estableciendo una cabecera de playa en un servidor que no estaba muy bien configurado.*

Pocos días después cuando el administrador logró cambiar la contraseña de su router, nosotros ya teníamos una manera de ingresar a su red salteándolo fácilmente desde dentro...”

5.2.- Los rasgos de un rol.

En las ciencias del comportamiento, cuando se estudia el comportamiento de los individuos dentro de un grupo, podemos observar que todo individuo asume un rol dentro del grupo. El ingeniero social explota esta característica, exhibiendo algunas características típicas del papel que interpreta, dejando que el blanco rellene los huecos. La mayoría de la gente tiene tendencia a completar la información basándose en unas pocas características (actitud, de comportamiento, apariencia, habla, etc.). Como dijimos previamente, el blanco inferirá el resto de las características, sin que el ingeniero social deba decir ni una sola palabra.

El siguiente ejemplo fue extraído del libro “El arte de la intrusión”^[KM02] de Kevin Mitnik: *“Un consultor contratado por un casino para testear la seguridad luego de sortear al guardia de la entrada, se presenta directamente en la sala de monitores de seguridad. La vestimenta del consultor es un traje azul, que por lo general lo visten los ejecutivos del casino. Los guardias lo miran con escepticismo y antes que nadie le pregunte nada dice con tono de autoridad:*

-Mirad a la mujer de la 12 –refiriéndose a la cámara 12, en todos los monitores aparecían mujeres- los guardias se agolpan frente al monitor de esa cámara tratando de determinar qué irregularidad estaría haciendo alguna de las mujeres que aparecen en el monitor”.

En realidad, los guardias, ante el hecho de un individuo vestido con traje (parecía un ejecutivo), con voz de mando y ya adentro del casino, asumieron inmediatamente que debía ser uno de los ejecutivos del casino haciendo una recorrida. Los guardias, en vez de pedirle su identificación como hubiera correspondido, llenaron los huecos de información y sin que el consultor dijese nada asumieron que era alguien con autoridad dejándolo pasearse libremente por las instalaciones.

5.3.- Lograr credibilidad.

Generalmente, desde el punto de vista de la víctima, éste el primer paso que ve. Establecer la credibilidad de su papel, es el paso más importante. Es el paso fundamental en el que se basa el éxito o el fracaso del ataque. Si el blanco cree en el ingeniero social, poco se puede hacer para evitar el ataque.

Según el Doctor Sagarin hay principalmente tres métodos a los cuales recurre un ingeniero social para establecer su credibilidad:

1. Peón sacrificado: El ingeniero social ofrece algo o aconseja en contra de sus propios intereses. Si lo viésemos como una partida de ajedrez, sería como sacrificar una pieza para lograr una posición mejor. El ingeniero social le diría a su blanco que ingrese la contraseña, pero que se fije que nadie lo esté mirando: *“Escribe tu contraseña pero no me la digas... Nunca debes decirle a nadie tu contraseña, ni siquiera a la gente de soporte técnico”*.
2. Vidente: El ingeniero social advierte que puede suceder algo que, sin que el blanco lo sepa, el atacante mismo lo ha provocado y lo va a provocar. En el libro El arte de la intrusión^[KM02] Kevin Mitnik pone un excelente ejemplo en dónde el atacante, informa a su blanco que habrá problemas con la red y que posiblemente se corte. Le pide al blanco que le diga cuál es el número puesto físico de la red; y luego engaña a administración de redes para que bloquee ese puesto.
3. El salvador: El ingeniero social soluciona el o los problemas que está sufriendo el blanco. Recordemos que, muchas veces, el atacante mismo genera esos problemas. El ingeniero social combina éste método con el anterior. El blanco no solo confirma su credibilidad, sino que le estará muy agradecido, y en deuda al atacante.

Veamos una anécdota que nos cuenta MasterCrack: *“Muchas veces, lo más difícil es lograr que te consideren una persona confiable. Que crean en ti. Una vez logrado, las llaves del reino se encuentran a tu alcance.*

Un tío, que trabajaba para una compañía de seguros, me había contratado para que le consiguiera acceso a la base de datos del Hospital Comunal. Apparently los tíos del hospital no habrían querido colaborar... Mejor para mí. Lo fácil que me fue hacer que el teclado fallara... je. Un pequeño tironcito y se desconectó. Esas tías no saben nada de máquinas... Le ofrecí ayuda y ni siquiera llamó a técnica. Mientras lo reconectaba, instalé mi pen-drive, que metió un troyano y a cobrar mis euros. La tía estaba tan agradecida, que hasta me invitó café. Después, desde esa máquina contaminé otras por las dudas... je.”

Si analizamos la anécdota vemos que el atacante, provocó un problema: una simple desconexión de un teclado. La falta de información de los usuarios puede hacer que un problema tan sencillo como un teclado desconectado sea un

problema insalvable. Y la falta de adiestramiento sobre los procedimientos hizo que, en vez de llamar a soporte técnico y esperar a que viniera personal calificado del hospital, una persona sin escrúpulos pudiera poner un programa troyano en la máquina, permitiendo el control de la misma desde Internet, por ende las historias clínicas de los pacientes quedaron expuestas a miradas no autorizadas.

5.4.- Lograr que el blanco asuma un rol.

El ingeniero social manipula al blanco para que adopte un rol alternativo, hacerlo pasar de sumisión a agresividad o, más generalmente, pasar de cualquier rol a uno que sea colaborativo. En el momento que el blanco asuma un papel de colaborador, es muy difícil que pueda salir de éste. Si comienza a colaborar, a ayudar, le resultará muy incómodo retroceder en su posición y negar la ayuda. Generalmente, el ingeniero social intentará que el blanco asuma un rol colaborativo solicitando pequeños favores que no exijan demasiado esfuerzo por parte del blanco. Luego se pasará lentamente al terreno que más le interesa para obtener la información o la ayuda que realmente busca del blanco que, si la hubiera solicitado de principio, posiblemente se hubiera encontrado con una negativa. Dado que el blanco ya está ayudando al ingeniero social, le será muy difícil, muy incómodo decirle que hasta allí llegó la ayuda.

El tema de brindar información es muy complicado dado que muy pocas organizaciones le dan la importancia suficiente y, lo peor, menos organizaciones transmiten esa importancia a los empleados que la manipulan, de manera que cuando alguien les solicita información, al darle poco valor a la misma consideran que el favor que les está pidiendo el ingeniero social “no cuesta nada”.

5.5.- Desviar la atención del pensamiento sistémico.

Si analizamos el pensamiento de los seres humanos, podemos observar que se dan dos formas de procesamiento:

- **Procesamiento sistemático o algorítmico:** la resolución de los problemas se realiza siguiendo una serie estricta de pasos racionales, en los cuales se consideran todas las posibilidades que se puedan presentar. Lógicamente las soluciones a las que se arriban de ésta manera son óptimas.
- **Procesamiento heurístico:** la resolución de los problemas se realiza utilizando “atajos mentales”. No se consideran todas las posibilidades sino que se aplican reglas dictadas por la experiencia y, por lógica, intervienen también los sentimientos de la persona. Las soluciones a las que se arriba de ésta manera no son necesariamente las óptimas, pero se llega a ellas con mayor velocidad.

Los científicos opinan que en cada ser humano, no se da ninguno de los procesamiento mencionados de forma pura. El procesamiento sistemático y el heurístico se entremezclan con diferentes grados según las personas y las situaciones. Otros sugieren que al no ser conscientes de todos nuestros pensamientos, lo que interpretamos como solución heurística podría deberse a un proceso algorítmico subconsciente.

El ingeniero social, buscará la manera de que su blanco procese la información mayormente de manera heurística, de forma que sus sentimientos tengan una influencia favorable para sus fines.

5.6.- Explotar el impulso de la conformidad.

El impulso de la conformidad podríamos asimilarlo a la primera ley de Newton, la ley de inercia: *En la ausencia de fuerzas exteriores, todo cuerpo continúa en su estado de reposo o de movimiento rectilíneo uniforme.*

Por lo general, las personas que tienen éste impulso de la conformidad (la mayoría), realiza las cosas de manera rutinaria. Los ingenieros sociales utilizan ésta debilidad cuando, por ejemplo, realizan un cuestionario. Siempre se comienza con preguntas triviales, generalmente de respuesta sencilla, y luego de unas cuantas preguntas, cuando el blanco baja la guardia y comienza a responder como rutina, se mechan las preguntas conflictivas, que el blanco responderá sin darse cuenta. De esa manera, los ingenieros sociales obtienen nombres de jefes, números de teléfono, correos electrónicos, nombres de usuarios, datos personales que pueden llevar a dilucidar contraseñas o, a veces, las mismas contraseñas.

Hay dos ejemplos de ésta debilidad en una vieja serie de televisión y en un testimonio sobre un hecho en la revisión médica del servicio militar.

El programa Columbo, se emitió regularmente en la década del 70 y actualmente puede verse en algún canal de cable. Era protagonizada por Peter Falk como el teniente Columbo, un detective de homicidios del Departamento de Policía de Los Ángeles que tenía una peculiaridad: sabía hacerse pasar por estúpido y hacía varias preguntas, muchas triviales, otras sin sentido, que hacían que el asesino fuera bajando la guardia; luego, al retirarse, lanzaba una última pregunta como que recién la recuerda y que generalmente es arrolladora: la respuesta siempre incriminaba finalmente al asesino.

Otro caso que se podría aplicar es uno que fue circulando de boca en boca y terminó formando parte del folclore de la revisión del servicio militar. Los convocados que intentaban salvarse por alguna enfermedad o algún problema físico tenían, luego de todas las revisiones médicas y presentación de papeles, una entrevista con una junta médica que era la que finalmente fallaba si el convocado era eximido del servicio o no.

Aparentemente, una vez apareció un convocado que presentaba un problema físico en la mano derecha: el dedo meñique siempre lo tenía cerrado. El convocado logró pasar con éxito los exámenes y cumplió con el papeleo (obviamente con certificados apócrifos), y terminó frente a la junta médica. Respondió impecablemente todas y cada una de las preguntas realizadas por los médicos. A tal punto que uno de los doctores dice que con la mano derecha en ese estado no podría sostener un arma, que debían eximirlo. Le lanza DNI (documento nacional de identidad) al convocado quien, totalmente desprevenido, trata de atajarlo en el aire moviendo el dedo “dañado” con total normalidad.

En los dos casos previos, se puede ver la aplicación de ésta debilidad utilizadas de manera constructiva. Por lo general, cuando lo utiliza un ingeniero social sin escrúpulos, puede ser devastadora.

5.7.- El deseo de ayudar.

Los psicólogos han identificado muchos beneficios que experimenta la gente cuando ayuda a otras personas. Ayudar nos hace salir del mal humos, nos hace sentir bien con nosotros mismos; y, aunque parezca mentira, ayudar nos hace sentir que tenemos el poder. El ingeniero social aprovecha esa inclinación del ser humano a prestar ayuda. Como hemos dicho con anterioridad, la gente no tiene conciencia del valor de la información, de manera que si prestar ayuda significa dar algo de información, consideran que el costo es bajo.

5.8.- Ganarse la simpatía del blanco.

Todos en alguna medida utilizamos esta técnica. ¿Cuántas veces nos ha sucedido que tenemos que realizar un trámite que puede durar mucho o que, quizás, no cumplimos con todos los requisitos y queremos apurar el trámite o tratar de que no presten atención al requisito que nos falta tratando de ser simpáticos y caerle bien al empleado que nos atiende? ¿Cuántas veces vemos que un/a adolescente (y a veces no tanto) hacer creer a la chica/o que les gustan, que escuchan la misma música, que tienen predilección por las mismas cosas?

Estos son usos bastante inocentes de la técnica, pero los ingenieros sociales que quieren perpetrar un ataque se aprovechan del hecho que todos tenemos más probabilidades de decir que sí a peticiones de gente que nos cae bien.

Muchas veces el ingeniero social deberá tratar que el blanco y él tienen los mismos intereses, o los mismos gustos, tratará de acariciar el ego del blanco con el fin de conseguir lo que quiere.

5.9.- Explotar el miedo.

Muchas veces el ingeniero social se sirve del miedo como si fuera una poderosa arma.

La explotación del miedo se puede realizar de dos maneras:

- El ingeniero social le hará creer al blanco que algo horrible sucederá; pero que podría evitarse si el blanco sigue las instrucciones del atacante.
- El ingeniero social toma un rol haciéndose pasar por un empleado de mayor autoridad. Son ataques basados en el estatus. El atacante puede hacerse pasar por directivo y dirigirse a un empleado de bajo rango (muchas veces se eligen como blanco de estos ataques a los empleados que parecen más novatos en la empresa) con la exigencia de “urgente”. El miedo al castigo queda implícito en esa exigencia.

5.10.- Explotar la reactancia.

La reactancia psicológica es la reacción negativa que experimentamos cuando sentimos que nos han arrebatado nuestra capacidad de elección o nuestras libertades.

Lograr que el blanco experimente reactancia es muy útil para el ingeniero social ya que el blanco pierde la perspectiva y quedaría a merced del manipulador.

Podemos aprovechar otra anécdota que me envió KnOwSeEk:

“Hace tiempo que tratábamos de entrar. Queríamos el código fuente de uno de sus juegos para poder hacer un keygen. Habíamos logrado tener datos de toda la red, nombres de servidores, logramos pispear alguno que otro usuario, pero jamás logramos romper ninguna de las contraseñas... Eran cuidadosos los guachos... Una vez, de casualidad, logramos capturar un email que enviaba uno de los jefes free-lance de proyecto, en dónde decía que se había mudado y daba su nueva dirección y teléfono... Fue un regalo caído del cielo. Con todo el conocimiento que teníamos de la red de la empresa, lo llamamos haciéndonos pasar por un empleado de Redes. Le avisamos que teníamos que hacer un reordenamiento de servidores y que por un par de días estarían fuera de servicio... Se los nombramos a todos... El tipo se enfureció y... (transcribe una serie de groserías) en una palabra dijo que era inaudito, que me costaría el puesto. Hice como que me asustaba y le prometí pasar todos sus programas a un servidor alternativo, pero que por favor lo mantuviera en secreto. Como quien no quiere la cosa le pedí su usuario y contraseña, para dejarle todo configurado... ¡Y me los dió! En unos minutos ya habíamos bajado el código fuente de casi todos los juegos de la empresa.”

Como puede observarse en éste ejemplo, el ingeniero social, jugó con la reactancia a fin de lograr que el blanco perdiera la perspectiva... y lo logró. La necesidad de recuperar su acceso aún no perdido hizo que el blanco perdiera la perspectiva y le dio al atacante lo que ellos llaman las llaves del reino.

6.- Un par de ejemplos prácticos e históricos

6.1.- El génesis y un mito egipcio

Qué mejor que iniciar el análisis de los casos prácticos con dos relatos históricos que, según los antropólogos estarían emparentados. El primer relato es un mito egipcio del siglo xii a.C., conocido como El Juicio de Horus y Set; sobre cómo Isis, madre de Horus, el hermano de Set, engañó a Set para que éste renunciara a su disputa con Horus por el trono.

El segundo relato, está sacado de la Biblia, el libro del Génesis Capítulos 25 y 27, sobre Jacob engañó a Esaú para quitarle la primogenitura.

Relato Egipcio

Luego de la muerte de Osiris, Set y Horus, peléan por el derecho a reinar sobre Egipto. Ra, forma un jurado con el consejo de Dioses y toma lugar lo que se conoce como el Juicio de Horus y Set.

Durante el juicio, Isis, madre de Horus, convence al resto de los dioses de que Horus debía heredar el trono. El único que no convencido fue Ra. Set, declara que no acatará ninguna decisión emitida por un tribunal que incluya a Isis. Ra instruye a los dioses para que se vuelvan a reunir en un lugar conocido como «la isla del Medio» y ordena al barquero que no deje cruzar a Isis ni a nadie que se le parezca.

La diosa se disfraza de vieja y le dice al barquero que lleva un plato de sopa para el joven hambriento que cuida el ganado. Su disfraz engaña al barquero y éste la lleva hasta la isla. Cuando pisa tierra, ve a Set y se transforma en una hermosa mujer.

Set, excitado, se acerca a ella. Cuando están juntos, ella le explica una historia muy triste. Su marido, dice, había sido un ganadero con quién ella había tenido un hijo. El marido se había muerto quedando el hijo a cargo el ganado, pero un extraño había entrado en el establo y había amenazado con golpear y expulsar al hijo y llevarse el ganado. Isis acaba pidiéndole protección a Set.

«¿Acaso mientras el hijo de un hombre sigue vivo —contesta Set— se le debe dar el ganado a un extraño?» Estas palabras de Set indican que la ley establece que el hijo tiene un derecho mayor sobre la propiedad de un padre que un extraño. Lo que no sabía mientras pronunciaba estas palabras, era que también estaba describiendo el conflicto legal entre él y Horus por el derecho a reinar en Egipto. Horus era hijo de Osiris, el anterior rey, y el reino le correspondía a su heredero, su hijo, y no a un rival. Inmediatamente después de pronunciar estas palabras, Isis se transforma en un pájaro y le grita que las propias palabras de Set le han delatado. Cuando Ra oyó lo que había dicho Set, declaró que Horus debía ser el rey...

Biblia – Génesis 25 y 27

Hizo un día Jacob un guiso, y llegando Esaú del campo, muy fatigado, dijo a Jacob, «Por favor, dame de comer de ese guiso rojo, que estoy desfallecido». Por esto se le dio a Esaú el nombre de Edom [es decir, «rojo»]. Le contestó Jacob: «Véndeme ahora mismo tu primogenitura». Respondió Esaú: «Estoy que me muero; ¿qué me importa la primogenitura?» «Júramelo ahora mismo», le dijo Jacob; y juró Esaú, vendiendo a Jacob su primogenitura. Diole entonces Jacob pan y el guiso de lentejas; y una vez que comió y bebió, se levantó Esaú y se fue, sin dársele nada de la primogenitura (Génesis 25, 29-34).

Cuando Isaac envejeció, sus ojos se debilitaron y perdió la vista. Llamó, pues, a Esaú, su hijo mayor, ...y mi alma te bendecirá antes de morir. Oyó Rebeca lo que Isaac decía a Esaú, su hijo... y Rebeca dijo a Jacob, su hijo... y se lo llevas a tu padre, que lo comerá y te bendecirá antes de su muerte. Contestó Jacob, a Rebeca, su madre: «Mira que Esaú, mi hermano, es hombre velludo y yo soy lampiño, y si me toca mi padre apareceré ante él como un mentiroso, y traeré sobre mí una maldición en vez de la bendición». Díjole su madre: «Sobre mí tu maldición, hijo mío; pero tú obedéceme. Anda y tráemelos»... Tomó Rebeca vestidos de Esaú, su hijo mayor, los mejores que tenía en casa, y se los vistió a Jacob, su hijo menor; y con las pieles de los cabritos le cubrió las manos y lo desnudo del cuello...y éste se lo llevó a su padre, y le dijo: «Padre mío». «Heme aquí, hijo mío», contestó Isaac. «¿Quién eres, hijo mío?» Y le contestó Jacob. «Yo soy Esaú, tu hijo primogénito. He hecho como me dijiste. Levántate, pues, te ruego:

siéntate, y come de mi caza, para que me bendigas»...y no le reconoció, porque estaban sus manos velludas como las de Esaú, su hermano, y se dispuso a bendecirle (Génesis 27,1-24).

Análisis de los casos

Dada la similitud, posiblemente el caso de la biblia sea una adaptación del caso egipcio (muy anterior), analizaremos los dos casos a la vez:

En el mito egipcio, al igual que en los versículos de la Biblia, se da que la jerarquía prefiere acepta que los derechos corresponden siempre al contendiente mayor y, en ambos casos, la madre prefiere al menor. En ambos casos, los originales de los derechos (Set y Esaú) son engañados para torcer el fallo en su contra y nuevamente en ambos casos, la madre es la ingeniera social. Veamos los principios involucrados:

En el caso Egipcio, la madre asume un rol (*aplicó el principio de agradabilidad y logró que el blanco asumiera un rol colaborativo*) de mujer bella en problemas y, utilizando un disfraz de mujer bella haciendo que Set se aleje del pensamiento sistémico (*Aplicó la búsqueda del pensamiento heurístico sobre el sistémico*), lo obliga a que tome el rol de protector-benefactor. En ese rol, Isis, logra que Set reconozca los derechos de su hijo, con lo que es condenado.

En el caso bíblico, Jacob, en primer lugar, aprovechando las necesidades de su hermano Esaú, Jacob negocia con él la primogenitura (*aplicó el principio de escasez*). Luego, siguiendo los consejos de su madre, se disfraza con las ropas de su hermano y asume el rol del mismo (*aplica los rasgos de un rol*).

6.2.- Entrada al partido de futbol.

Esta anécdota me la relató un muchacho que lo llaman Pelo.

Pelo es un hincha fanático del equipo A de futbol. En un partido considerado uno de los clásicos, jugaba el equipo A contra su archienemigo B en una final. Lógicamente las entradas se agotaron casi inmediatamente y Pelo no consiguió ninguna.

El muchacho no se desanimó y el día del partido, se vistió con un traje y se dirigió a la cancha.

Primero se paseaba junto a la fila de hinchas que esperaban la revisión de rigor, y poder ingresar al estadio. Llegó antes que permitieran la entrada. Notó que varios guardias lo observaban, pero luego de un tiempo, perdieron interés en él. Se acercó a uno de los jefes de guardia, y con un cuentaganado, de esos baratos que venden en las tiendas de chucherías, se puso a hablar con un dejo de autoridad.

-Justo hoy tenía que hacer tanto calor... con las pocas ganas que tengo de trabajar -le dijo al encargado y antes de que el hombre le respondiera agregó - ¿ya bloquearon el paso entre la dos y la tres? Espero que no vuelvan a romper el alambrado.

-Hay quince guardias en la zona.

-Sobran.

-Espero que sí -agregó el encargado.

A medida que se acercaba el momento de la apertura del portón de locales, saludando a uno y a otro, con el cuentaganado sostenido de manera visible en la mano, se puso a un costado de la puerta junto al guardia.

Cuando abrieron la puerta, el se puso a contar con el cuentaganado a los hinchas que iban entrando. Aún no intentó entrar.

Cuando ya habían ingresado más de la mitad de los hinchas, le entrega el cuenta ganado al guardia.

-Podés darme una mano. Este traje y el calor me están matando. Tomo un trago de agua y vuelvo.

-Metete pata que si me ven me pueden llamar la atención -le responde el guardia. El muchacho, en vez de ir a uno de los vendedores ambulantes, se dirige a uno de los micros que trajo a los de seguridad. Saludando con cortesía y caminando con firmeza, tomó uno de los vasos descartables del “dispenser” que había al lado del vehículo y sin tomárselo del todo volvió a su “puesto”.

-Gracias. ¿Querés un trago? -le ofrece al guardia que lo acepta sin decir palabra. Luego de un rato, comienza a moverse incómodo y vuelve a dirigirse al guardia:

-Disculpame. Es la primera vez que me toca estar en los portones, tanto líquido y tanto calor (Pelo sabía perfectamente que el baño más cercano se encuentra bajo las gradas dentro del estadio). ¿Dónde está el baño más cercano?

El guardia, sin decirle nada extiende la mano para que le dé el cuentagano y con la otra mano le señala dentro del estadio.

Caminando con tranquilidad Pelo entró el estadio y se dirigió directamente hacia el alambrado al borde del campo de juego desde donde pudo ver todo el partido. Nadie le preguntó ni le dijo nada.

Análisis del caso

No todos los casos de ingeniería social tienen cabida en el medio informático. En realidad la mayoría de los ataques de ingeniería social se dan fuera del ámbito informático. El problema que los casos más devastadores y más publicitados son los que tienen que ver con los ataques a redes de computadoras y a sistemas.

Como podemos ver en este caso, Pelo asumió un rol de trabajador. Como podemos ver, primero se paseó con autoridad del principio al final de la fila de hinchas. El estar vestido con un traje en vísperas de un partido de fútbol, hizo que los hinchas pensaran que era alguien de seguridad... y evidentemente, los guardias pensaron parecido. Buscó afianzar su credibilidad hablando con el jefe de los guardias de seguridad, utilizando comentarios con autoridad (*aplicó el principio de autoridad*). Los guardias que lo vieron hablando con su jefe, ya asumían que Pelo podía ser o alguien de seguridad dentro de su equipo o algún supervisor (tema que el reforzaba dejando ver el cuenta ganado -*aplicó el principio de autoridad, con los rasgos de un rol*-).

Ya el haber llegado al costado de la puerta, junto al guardia de seguridad, probaba que su credibilidad había sido aceptada. Para no levantar sospecha y afianzar su posición. Hizo la jugarreta del agua. El guardia aceptó ayudarlo mientras él, inocentemente, tomaba un trago de agua (*aplicó el principio de agradabilidad y logró que el blanco asumiera un rol colaborativo*).

Cuando Pelo, nuevamente le pide otro favor, al guardia seguramente le resultaba incómodo decirle que no y, no solo aceptó ocuparse del cuenta ganado, sino que dejó entrar al muchacho al estadio para que pudiera ir al baño (*aplicó el principio de consistencia y explotó el impulso de la conformidad*).

6.3.- El vecino molesto.

Este caso me lo ha enviado un Gerente de fábrica de una empresa manufacturera de la Ciudad Autónoma de Buenos Aires:

Soy el gerente de fabricación de una empresa manufacturera inserta en el corazón de la Ciudad de Buenos Aires. Si bien en la empresa tratamos de respetar todas las disposiciones vigentes, reconozco que el bienestar de los vecinos nunca fue una de nuestras prioridades.

Durante el año pasado, sucedió que una de las estampadoras, tenía el sistema de amortiguación defectuoso, de manera que cuando el enorme pistón moldeaba las chapas, la vibración y el ruido salían fácilmente de la fábrica. Recuerdo que estábamos muy apretados de tiempo y decidimos extender el horario de fabricación hasta bastante entrada la noche.

Los partes de seguridad señalaban varias llamadas telefónicas nocturnas solicitando que dejáramos de hacer ruido. El gerente de seguridad, que participaba en todas las reuniones operativas, sabía del problema de tiempos que teníamos y decidió no prestar atención a esos reclamos.

Al tercero o cuarto día, recibí una llamada en mi domicilio particular, aproximadamente a las tres de la mañana, con una buena retahíla de insultos por el ruido que producíamos. Seguido a ese llamado, casi hasta las cinco de la mañana, uno tras otro llamaron muchos de los vecinos de las inmediaciones de la fábrica.

Cuando al otro día llegué a la fábrica, habían programado una reunión de urgencia: casi todos los gerentes, incluso los directivos, habían recibido llamadas similares y estábamos todos bastante furiosos.

La gerencia de seguridad, comentó en la reunión las llamadas de queja de los vecinos. Se le ordenó a la gerencia de seguridad el averiguar cómo se había producido la filtración de la nómina de jerárquicos de la empresa.

A continuación transcribo algunos párrafos que pueden dar un poco de luz sobre la falla de seguridad:

“El día xx de junio a las 8:00 AM (la mañana siguiente a la primer jornada extendida), se apersonó en ésta guardia, un cadete en moto. El mismo venía con ropas similares a la que utilizan los vigiladores. Dijo provenir de la empresa de seguridad y que lo enviaba el jefe de relaciones públicas a buscar un sobre. Es una operatoria muy común. A veces se llevan copias de los partes para una auditoría, otras se llevan los libros de movimientos llenos y traen los vacíos. Buscan las listas con los turnos de guardias, etc.

Los vigiladores buscaron el mencionado sobre sin hallarlo. Ante la pregunta de los mismos sobre qué contenía ese sobre, el cadete respondió: Debería tener un listado con los nombres y los teléfonos de los jefes... Me dijeron que estaba preparado... ¿A ustedes no les dijeron nada? Me parece que el jefe se va a calentar bastante.

Los vigiladotes, sin darle suficiente importancia a la información. Tomaron el listado de llamadas de emergencia (que contiene los datos de ubicación de todos los jerárquicos, detallada por sector, incluyendo a los directivos), le sacaron una fotocopia, la pusieron en un sobre, y se la entregaron al cadete. En el libro de movimientos, simplemente pusieron:

Junio xx, 8:00 AM Cadete retira el sobre para YYY...

Consultando a los vecinos (estaban enojados y muchos nos cerraron la puerta en la cara), nos comentaron que ayer por la tarde, dejaron una copia de la lista por debajo de la puerta con una nota que decía:

La única manera que dejen de hacer ruido es que llamemos directamente a los jefes y los despertemos a la hora que nos despiertan.

La nota estaba escrita con una computadora e impresa en una impresora a chorro..." (Continúa con detalles sin importancia)

Análisis del caso

Como hice en todos los casos del presente trabajo, YYY representa el nombre de la empresa de seguridad.

En éste caso, falta un detalle en el informe. Dado que muchas veces los vecinos se han quejado, han podido establecer muchos puntos, que para uno de los vecinos entrenados le dio el conocimiento previo sobre la fábrica, su modus operandi, y su jerga (en realidad la jerga de los vigiladotes es bastante común y similar en todas las empresas de seguridad). Según me dijo el Gerente de fabricación, la lista se encuentra clavada con chinchas al lado del gabinete de seguridad; visible (pero no legible) por cualquiera que se acerque a los de seguridad para hacer una pregunta o una queja.

Evidentemente la nota se obtuvo utilizando un ataque de ingeniería social. Se utilizó el conocimiento de la cultura y estructura de la empresa de seguridad para establecer la *credibilidad utilizando los rasgos de un rol*, se utilizaron amenazas veladas en la aplicación del *principio de autoridad*.

Por otra parte, el ingeniero social ofreció a los vecinos una solución al problema del ruido nocturno que no entrañaba mucho esfuerzo y que permitiría desahogar sus broncas (*El principio de la reactancia* –le quitaron horas de sueño, y quieren recuperarlas).

Cuando le pregunté al ingeniero sobre si no reconocieron al muchacho de la moto, reconoció que durante un tiempo tuvieron a los dos vigiladotes caminando por la calle a ver si reconocían a alguien, pero sin duda debieron utilizar a algún amigo o conocido que no vive por la zona. Por otra parte decidieron no continuar con el tema ya que, en realidad, los que estuvieron actuando desaprensivamente con los vecinos, fueron ellos.

6.4.- Test de penetración.

Este es el único caso que puedo asegurar su veracidad ya que he visto actuar a la empresa de seguridad a la que representa el consultor CISSP que me brindó el siguiente relato.

Hace aproximadamente un año, he sido contratado por una compañía de seguros para realizar un test de penetración no sólo de sus sistemas informáticos sino también de la seguridad física del edificio central.

A fin de evitar problemas legales, se firma un contrato de confidencialidad y carta blanca, en el cual nos comprometemos a mantener toda la información que obtengamos en secreto y la empresa nos otorga un permiso para que tratemos de penetrar en sus sistemas sin que ello constituya delito.

Tenemos un procedimiento bastante efectivo, que nos permite mantener una coherencia de la información que vamos obteniendo.

Primero, el equipo de información previa obtiene toda la información que Internet nos pueda brindar de la empresa objetivo como proveedores, sucursales, servidores, redes, etc.

Seguidamente, el equipo de *pentest* “Penetration testing” (test de penetración) busca todas las vulnerabilidades e intenta tomar el control de los servidores y de las redes. Este es un equipo de verdaderos Hackers éticos y es de operación estrictamente técnico.

Mientras tanto un segundo equipo se encarga de tratar de ingresar al los diferentes sectores de la empresa y obtener información que pudiera ayudar al equipo técnico (como usuarios, contraseñas, etc.)

Dado que mis conocimientos técnicos son pobres, formo parte del segundo equipo.

Lo primero que hice es pasarme algunos días en el bar junto a la empresa, dónde los empleados normalmente desayunan y almuerzan. Armado de una grabadora digital, trato de escuchar y grabar todas las conversaciones de empleados de la empresa, fácilmente ubicables por las identificaciones prendidas de sus bolsillos. De las conversaciones, fuera de tratar de buscar indicios de información relevante como nombres de jefes, reputaciones, apodos, etc, se obtiene una buena idea de la jerga que utilizan los empleados de la compañía. Como en todas las organizaciones, uno de los elementos culturales distintivos es la manera de hablar

y las palabras que utilizan (la jerga). El saber la jerga, te abre muchas puertas y te saca de muchos apuros. Así aprendí que *Narices* es uno de los soportes técnicos y que es bastante tarambana; que el *Jegarca* es el jefe del departamento de recursos humanos; que los de compras se mandaron una macana bastante grande con una compra “arreglada”, etc.

En el mismo bar, ya comencé a establecer relaciones con empleados de la empresa, hablando con chicos de sistemas (son inconfundibles por su cháchara técnica) del problema de compras, con los de compras de las torpezas de Narices, de que el *Jegarca* me llamó por mis llegadas tardes, etc.

Seguí ese jueguito durante una semana. Muchos empleados ya me conocían y me saludaban apenas entraba.

Discretamente, otro de los muchachos de mi equipo, armado de una buena cámara digital saca la mayor cantidad de fotografías posibles a las identificaciones que portan los empleados de la empresa. Luego, cuando crucemos información antes del ataque físico, haremos copias de las identificaciones con nuestras respectivas fotografías.

A los diez días llegó el día D hora cero. La prueba de fuego, entraría en la empresa. El ataque físico a través de la puerta de empleados lo haría yo, mientras, por la puerta de clientes lo intentarían dos compañeros de equipo.

Lo más difícil es pasar a los de seguridad.

Munido de un currículum vitae (obviamente falso), con una identificación celeste en un bolsillo y con una copia de la carta blanca en el otro (para evitar problemas si fracasaba en mi intento). Mostrando nerviosismo y timidez me acerco lentamente al mostrador de seguridad. Muestro indecisión dejando pasar a dos muchachos que querían averiguar algo. Mientras memorizo la posición de las oficinas en el tablero detrás del mostrador de seguridad.

(Guardia): ¿En qué lo podemos ayudar?

(Yo): Ehhh... Me llamaron de recursos humanos para que... trajera mi currículum... Soy programador... Estoy buscando empleo.

(G): Es en el tercer piso. (Aparentemente el guardia, una persona mayor, se apiadó del muchacho que busca trabajo y se siente muy nervioso) Pero arriba ese ánimo. Si querés que te contraten tenés que mostrarte más enérgico. Cuando hables con los entrevistadores, que no se den cuenta que tenés miedo (me dice mientras copia el nombre de mi currículum en la computadora).

(Y): Es... difícil.

(G): (Hablando bajito y en confidencia) Te comprendo, pero yo no te dije que están desesperados por la falta de programadores (y me da una identificación de invitado mientras me guiña un ojo)

Con una tímida sonrisa acepto la identificación y me dirijo hacia el ascensor de empleados. Dejo subir a dos empleados en uno de los ascensores, mientras se abre la puerta del segundo. Subo en él solo.

Una vez en el ascensor, cambio la identificación verde de invitado por una identificación celeste de empleado: Ya estaba adentro.

Podía ir a cualquier piso, excepto el primero. Allí está auditoría, quienes me contrataron y me conocen.

Decido ir primero por compras, que queda en el mismo tercer piso que recursos humanos.

En la oficina de compras había diez empleados. Estaban todos sentados en sus escritorios. Por suerte parece que no había nadie de auditoría. Se les notaba abiertamente desanimados. Una empleada, la más cercana al mostrador, se acerca mirando mi identificación.

(Empleada): ¿En que puedo ayudarlo?

(Yo): Soy de auditoría (noto que todos me miran con odio). Bueno, recién me pasaron a auditoría y quería saber si estaba acá mi jefe.

(E): No. Hoy, aún no ha venido.

(Y): Huy, dónde estará, me pidió que tomara unas fotografías para no se qué expediente.

(E): Hagan lo que quieran. Total, estamos condenados (Me dice mientras se vuelve a su escritorio).

Cuando tomo algunas fotografías con mi cámara todos bajan las cabezas. Realmente me dio lástima, pero debo hacer mi trabajo. Ya tengo mi primer éxito. Ingresé a una de las oficinas y nadie me detuvo.

Mi segundo éxito fue en el quinto piso: Oficina de riesgos. Les dije que estaba destinado a una oficina del interior y estaba viendo cómo se mueven en la central. No sólo no me detuvieron sino que me explicaron, con lujo de detalles, cual era su trabajo. Hasta posaron conmigo para las fotografía.

Decido ir por uno de los premios mayores: sexto piso, sistemas. Entro en el piso observándolo todo. Me acerco hacia el nicho hidrante (donde se ubica la manguera de incendios), golpeo suavemente el vidrio con el revés del anillo, anoto algo en el revés de mi currículum vitae. Me acerco a uno de los matafuegos, miro la etiqueta y vuelvo a anotar, saco una fotografía de la puerta, otra del plano de evacuación. Los empleados que están a la vista me observan, pero nadie me dice nada. Saco una fotografía hacia los cubículos. De una oficina detrás de paneles de vidrio, se acerca a paso rápido un señor.

(Yo): Buenos días (lo atajo estirando la mano). Soy de higiene y seguridad –le digo estrechándole la mano. ¿con quién tengo el gusto?

(Juan): Soy Juan xxx Jefe de tecnología. No me dijeron nada de una inspección.

(Y): ¿*Jegarca* no les avisó? (Moviendo la cabeza agrego) ¿Porqué no me extraña? Acabo de venir de GG (como le dicen a gerencia general) y allí tampoco habían avisado.

Entran dos programadores con los que estuve hablando en el bar y me saludan mostrando que me conocen (cayeron del cielo). Antes que Juan continuara, me explico:

(Y): Tenemos intenciones de cambiar el sistema antiincendios y estoy haciendo un relevamiento para saber dónde estamos parados. Soy un poco nuevo en la compañía y me vendría bien un poco de ayuda. ¿puede mostrarme los equipos?

(J): Comprendo... acompañeme.

El tema es que el mismo jefe de tecnología me acompañó a todas las dependencias de sistemas mostrándome todos los elementos de seguridad. Y explicándome todo lo que veía. Incluso me permitió sacar fotografías a los equipos centrales. Cuando ya me estaba yendo, me mostró la pequeña sala en donde se encuentra el *gabinete de comunicaciones*. Mientras me explicaba la cantidad de equipos que se interconectan, puedo ver, amurado, un *access point* inalámbrico que tenía un rótulo pegado que decía SDCI01 – 10.0.0.34 – admin 53er3dd (un verdadero regalo para los chicos de pentest).

Realmente la primera y única incursión que hice fue un éxito, pero no quería irme sin intentar acceder al premio mayor: Gerencia General, el piso 11.

Apenas se abre la puerta del ascensor, un guardia de seguridad, mira mi identificación y me pregunta qué deseo.

Le digo que soy de relaciones públicas, que tenemos una buena posibilidad de publicar y que necesitaba un par de fotografías del jefe.

Sin decir nada apunta su dedo hacia la secretaria.

(Secretaria): Buenos días.

(Yo): Hola, soy de relaciones públicas. Necesitaría tomarle unas fotos a GG para el concepto de una publicidad.

(S): No tiene cita.

(Y): No, no la tengo. Pero consúltelo, no le voy a robar más que unos segundos.

La secretaria contrariada, en vez de corroborar mi historia, llama a su jefe y le pregunta. En menos de cinco minutos (tiempo que aproveché par tomar algunas fotos), el GG me estaba abriendo las puertas de su oficina. Saqué fotos de la oficina y del GG posando con sonrisa de plástico en su escritorio, sentado en su sillón concentrado en unos papeles, y hablando por celular. Cuando presentara mi informe, me podría jactar de haber logrado el premio mayor.

Por otra parte, el equipo de *pentest*, con los datos del punto de acceso inalámbrico, logró *esnifear* varias conexiones inalámbricas obteniendo usuarios, contraseñas de alto nivel.

Análisis del caso

Este caso es tan largo como complejo. Este profesional, ha utilizado casi todos los principios de influencia y podemos ver claramente muchos de los pasos enunciados en el punto anatomía de un ataque.

Primeramente, el ingeniero social se hace ver en el bar que frecuentan los empleados y comienza a tomar contacto con ellos y estudia su cultura (*conocimiento del objetivo*). Seguidamente se falsifican las identificaciones a fin de que el Ingeniero social pueda pasearse dentro de las instalaciones de la empresa sin mayores problemas (*rasgos de un rol*). Con la semana de charlas informales previas con distintos empleados de la compañía en el bar, estableció una suerte de *credibilidad* de que es empleado.

También mostró los *rasgos de un rol* cuando se paseó por sistemas tomando notas interesándose sólo del material antiincendios.

Para ingresar por seguridad sin que le pidan documentos (cosa que deberían hacer), el ingeniero social hace que el guardia *asuma un rol colaborativo* y paternalista *desviándolo del pensamiento sistémico*. En vez de pedirle una identificación, simplemente copia el nombre del curriculum vitae. Lo mismo logró con el gerente de tecnología, pidiéndole que lo acompañe y le muestre los equipos.

Cuando ingresa en compras aprovecha los problemas que tienen y asume un rol de autoridad (*principio de autoridad*), lo mismo hace cuando le nombra al gerente de tecnología al gerente general y al jefe de recursos humanos.

6.5.- Blanco en el Foro.

Éste es un relato que he recibido por email hace un tiempo. Sé distribuyó por la red de habla hispana como cadena de correo electrónico, no puedo asegurar su veracidad, pero contactándome con algunos organismos oficiales, es posible que sea cierta.

NOTA: Como casi todos los casos que se relatan en el presente trabajo, aunque su veracidad no haya sido probada, lo ponemos como caso didáctico.

A nuestro ingeniero social lo llamaremos Don X. Es un sociólogo funcionario de una oficina de protección del menor y con 30 años capitanea un grupo de prevención extraoficial.

Los objetivos de éste grupo es concientizar a los padres sobre lo importante que es que los niños tengan un control estricto y estén perfectamente educados para evitar dar información a gente que pueda usarla para perjudicarlos.

Don X se conecta asiduamente en algunos foros de adolescentes y toma varias identidades de ambos sexos, gracias al anonimato imperante en los mismos. De

esa manera se mantiene al tanto de la problemática, interés y gustos de los chicos a los que debe proteger. Como objetivo secundario, cuando encuentra algún menor especialmente vulnerable que pueda encontrarse en riesgo, busca la manera de tomar contacto de una manera oficial.

Este fue el caso de una niña llamada Sonia que decía tener 12 años y que se mostraba demasiado comunicativa y provocaba a los muchachos con insinuaciones bastante abiertas.

Don X decidió seguirla un poco de cerca y, en ese foro, tenía dos identidades: Ricardo y Alicia, aproximadamente fingía una edad cercana a la de Sonia.

Luego de estar estudiándola un poco, por los mensajes suponiéndolos parcialmente verdaderos y cruzando unos con otros (esto último puede realizarse muy fácilmente ya que la mayoría de los foros tienen algoritmos buscadores que permiten ver todos los mensajes que un determinado usuario envía), DonX pudo deducir lo siguiente:

- Efectivamente pertenecía a un rango de edades entre 11 y 13 años.
- Formaba parte de una familia acomodada.
- Era hija única.
- La música que le gusta
- Como casi todas las niñas a esa edad muestran cierta rebeldía, pero no parecía llevarse mal con los padres.
- Asistía a un colegio privado.
- Practicaba hockey sobre césped y casi siempre estaba al arco.
- Casi todos los jueves se encuentra sola en casa porque es el día que sus padres salen solos.

Entre otras cosas.

Don X decidió que su personaje Alicia, asumiera el rol de chica rebelde y que andaba detrás de Ricardo.

De una manera lenta pero firme, “Alicia” logró una amistad electrónica con Sonia y ésta le ayudaría con Ricardo; mientras tanto, entre conversación y conversación, Alicia logró la siguiente información:

- El colegio era un colegio religioso.
- Su padre era un empresario
- El barrio al que pertenecía y que vivía a seis calles del colegio
- Que era alta y su cabello, castaño.
- Martes y jueves tenía hockey
- La madre era ama de casa
- Que caminaba desde el colegio a su casa con una compañera.

Don X ya tenía la suficiente información para poder ubicar a la niña y decidió probar suerte. Fue al colegio un martes y se quedó vigilando desde un bar en una

esquina para poder determinar el horario de las prácticas de hockey. A las once de la mañana, un grupo de chicas salieron a precalentar con los palos de hockey en la mano. Don X se dirigió al colegio con la excusa de que tenía una hija de cinco años que al año siguiente iniciaría la primaria que quería ver las instalaciones del colegio. La vicedirectora en persona le hizo un recorrido, y él se detuvo especialmente en las gradas mientras las chicas jugaban hockey pudo distinguir sin problema a la niña que en el Foro se hacía llamar Sonia. Una de las niñas al arco tenía pelo azabache mientras que la otra tenía cabello castaño. Sólo que los niños la llamaban Bea (seguramente su verdadero nombre era Beatriz). Mientras esperaba que la niña se sacara el protector para poder reconocerla luego a la salida, la vicedirectora no paraba de hablar sobre las bondades del colegio y la elección del hockey como deporte de elite, etc. El partido llegó a un entretiempo y la niña se quitó el protector y nuestro ingeniero social pudo ver la cara de su blanco.

Don X le agradeció a la vicedirectora y prometiéndole volver luego de hablar con su esposa, la saludó a la espera de la salida de los niños.

Don X esperó tomando un refresco en el mismo bar que antes hasta la salida de los niños. El resto fue tan simple como caminar cinco cuadras a una distancia respetable y ver a qué casa entraba la niña.

Mirando hacia la cochera de la casa, podía verse la parte trasera de un Mondeo. Seguramente el padre también estaba en casa.

Don X, con una carpeta con parte de las conversaciones y todas las deducciones bajo el brazo, tocó el timbre de la casa. Lo atendió una mujer muy parecida a la niña (evidentemente su madre). Explicándole muy brevemente su trabajo y el trabajo del grupo que capitaneaba, la mujer lo dejó entrar. La mujer llamó a su marido y con él apareció también la niña.

Don X dejó a esos padres azorados por la información que obtuvo de las conversaciones inocentes de su hija (decidió dejar las provocaciones de lado ya que no servían a sus fines). Por la cara aterrada de la niña ella captó el mensaje. Les comentó que si fuera un delincuente sabría lo suficiente para poder asaltar (o cosas peores) sin mayores problemas. Que era muy importante evitar a toda costa dar cualquier tipo de información, y dado que eso es bastante complicado para un adolescente, que debía evitar utilizar los servicios de foros anónimos y sólo comunicarse con conocidos.

Análisis del caso

Este caso es realmente preocupante ya que como padres es bastante difícil educar a los niños sobre la importancia y el valor de la información. Como todos sabemos vivimos en una sociedad enferma en donde los asaltantes,

secuestradores y violadores tienen acceso a un caudal de información que puede facilitarles mucho la tarea.

Lo primero que observamos en el caso es la importancia de recabar la mayor cantidad de información posible sobre el blanco. En éste caso el pez por los dedos muere. La niña, si bien da información falsa, un ojo entrenado y con tiempo suficiente sabrá cruzarla podrá obtener datos verdaderos de la maraña de cuentos y exageraciones.

Luego de tener información suficiente, aplicó los *rasgos de un rol* para que la niña le confiara más información a otra que tenía problemas con un chico que no le prestaba atención (*hacer asumir un rol colaborativo al blanco*).

Si le prestamos mayor atención al caso, la madre también fue presa de un ataque de ingeniería social. Don X jamás mostró credencial alguna. Simplemente, con algunos datos estableció su *credibilidad* y su presentación más la tenencia de un “expediente” bajo el brazo, asumió los *rasgos de un rol* frente a la madre que lo dejó entrar en la casa sin ningún problema.

7.- Cómo protegerse de un ataque de ingeniería social

El poder protegerse de los ataques de ingeniería social es un asunto estrictamente cultural. La educación es la única arma verdadera. La educación y protocolos de seguridad cuidadosamente implementados.

Vamos a analizar los protocolos de seguridad en dos ámbitos: en el ámbito doméstico, y en el ámbito organizacional.

Curiosamente es una cuestión de escala.

En el ámbito doméstico, cada llamada telefónica recibida de personas desconocidas, deben ser especialmente escuetas. Cuánto más se habla, más información se da, y cuanto más información se da, más riesgo se corre. En el ámbito doméstico es un poco más simple ya que teóricamente conocemos a todos nuestros familiares.

¡Qué sucedería si como en uno de los relatos en el punto anterior, vamos a nuestro living y encontramos a un desconocido paseando por ahí. Lo primero que vamos a exigir es que se identifique, y seguidamente, antes de echarlo de mala manera, le preguntaríamos que está haciendo. Ésta es la parte fácil. La parte más difícil es mantener una conducta discreta frente a los desconocidos.

Los niños en las casas son siempre los blancos más fáciles y entrenarlos para que no den información, sobre el valor y los peligros de dar información, es lo más complicado.

Una herramienta poderosa como es la computadora e Internet con su correo electrónico, la mensajería instantánea y los foros, no debe quedar sin control cuando la utilizan niños. Observen el último caso analizado: cómo una niña observada y manipulada por un profesional, dio suficiente información para que un delincuente pudiera penetrar en la vivienda en el momento que menos resistencia habría, cuando la niña está sola o secuestrarla en la ida a vuelta del colegio, o cosas peores. Sin duda que esas cosas podrían pasar al azar, pero para que entregar información y dejar que se planifiquen los delitos.

En el ámbito organizacional, primero se deben tomar medidas tendientes a fortalecer la seguridad y luego educar a los empleados para que las sigan sin dudas.

Sin duda es imprescindible que los altos cargos comprendan la importancia y apoyen todas las iniciativas tendientes a mejorar la seguridad de la información.

Lo primero que debemos hacer es definir los protocolos de seguridad que se deben aplicar obligatoriamente en todo el ámbito de la organización.

Las normas deben ser sencillas y fáciles de seguir. Las acciones por omisión es denegar. Todo lo que no está estrictamente permitido debe estar prohibido.

Veamos algunas acciones directas que deben grabarse a fuego en los empleados:

- Debe concientizarse a los empleados sobre la importancia y el valor de la información.
- Siempre que se vea a un desconocido en un área restringida, debe pedirse identificación.
- Debe denegarse el paso a toda persona que no esté perfectamente identificada a áreas restringidas
- Las áreas de atención pública deben estar especialmente separadas de las áreas restringidas
- Modificar las normas de educación de manera que para ceder el paso a un ascensor, mantener una puerta abierta para que pase una persona, la misma debe estar perfectamente identificada.
- Debe dejarse perfectamente en claro y con normas sencillas, la clasificación de la información entre pública, restringida y confidencial
- Como todos los sistemas de seguridad, debe testearse periódicamente la permeabilidad de los empleados a los ataques de ingeniería social. Estas pruebas mantendrán alertas y entrenados a los empleados.
- Educar, educar y educar a los empleados. Castigarlos y sancionarlos, no siempre son la mejor opción (generalmente es la peor) cuando un empleado es víctima de un ataque de ingeniería social, debe ser educado, educado y educado. Debe tenerse en cuenta que el empleado que cae víctima de un ataque de ingeniería social probablemente sienta la suficiente humillación para evitar que le vuelva a suceder.
- Debe documentarse todo incidente tanto exitoso como frustrado y publicado para que todos los empleados estén alertas.
- Debe entrenarse a los empleados que cuando sospechan un posible comienzo de ataque de ingeniería social, debe darse parte inmediato al personal de seguridad sin temor a que sea una falsa alarma.

Glosario

Access point	Punto de acceso en inglés. Es un equipo que conecta los equipos inalámbricos entre sí y a una red cableada. Son equipos complejos que permiten encriptación y seguridad, pero no siempre están bien implementados.
Esnifear	Es un neologismo que se utiliza en el ámbito de las redes informáticas, para conectarse a una red y analizar la totalidad de los paquetes de información que pasan por ella. Con ésta técnica se puede revisar toda la información que circula por la red.
Foro	Sitio web interactivo utilizado por muchos internautas para intercambiar opiniones, mensajes y ayuda sobre ciertos temas de interés. Hay foros hacker, foros de cocina, foros de programación, foros esotéricos, foros de ciencia ficción, etc.
Keygen	Es un programa que sirve para generar claves que permitan hacer que un juego, obtenido de forma pirata o en su formato shareware, funcione como un original completo.
Keylogger	Es un programa que originalmente se desarrolló como herramienta de diagnóstico. El programa tiene como objetivo almacenar todas las pulsaciones del teclado. Dada la enorme potencia de la herramienta para el espionaje, actualmente hay un gran número de ellas, con tecnología de ocultamiento, que utilizan los crackers para obtener usuarios y contraseñas. Ver jargon file ^[JF01]
Messenger	Grupo de programas que utilizan los internautas para comunicarse utilizando la red Internet. Dado que, normalmente, se utiliza el teclado, y los mensajes son de texto, suele suceder que los interlocutores no se conozcan físicamente.
Pen-drive	Es un dispositivo de hardware compuesto por una memoria de tamaño pequeño y gran capacidad que generalmente se conecta a un puerto USB y que el sistema operativo lo reconoce como una nueva unidad de disco y se puede operar como tal.
Pentest	Es una contracción de penetration testing (test de penetración) es el uso de técnicas de hackin para analizar las vulnerabilidades de un sistema informática (entendiendo por sistema tanto al software, como al

	hardware y las redes)
Router o enrutador	Enrutador (router), ruteador o encaminador es un dispositivo de hardware para interconexión de red de computadoras que opera en la capa tres (nivel de red). Este dispositivo permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.
Shareware	Programas que se entregan a través de Internet a modo de demos jugables. Luego, con la introducción de una contraseña, se obtiene acceso a todo el programa.
SPAM	Se llama SPAM o correo basura a todo mensaje no solicitado que recibe un usuario de correo. Por lo general son mensajes publicitarios, aunque algunos son virus.
Spyware	Son programas espía que se alojan en una máquina y recopilan información de una máquina o de una organización sin consentimiento de los propietarios, y luego envía esa información a través de Internet.
Troyano	Los troyanos son programas maliciosos que se instalan en una computadora y que funcionan como puerta de entrada a usuarios externos no autorizados por el propietario. Los programas troyanos más conocidos son el backOrifice, Bifrose, NetBus y Subseven.
Wikipedia	Es una enciclopedia libre políglota basada en la tecnología wiki . Wikipedia se escribe de forma colaborativa por voluntarios , permitiendo que la gran mayoría de los artículos sean modificados por cualquier persona con acceso mediante un navegador web .

Referencias

-
- [W101] http://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_%28ciencias_pol%C3%ADticas%29
 - [W102] http://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_%28seguridad_inform%C3%A1tica%29
 - [SG01] Sara Granger – Social Engineering Fundamentals, Part I: <http://www.securityfocus.com/infocus/1527>
 - [MA01] Jorge Machado <http://www.perantivirus.com/sosvirus/pregunta/ingsocial.htm>
 - [KM01] Kevin Mitnik y William Simon – The art of Deception: Controlling the Human Element of Security – Wiley Publishing Inc. – Año 2002
 - [KM02] Kevin Mitnik y William Simon – El arte de la intrusión: Cómo ser un hacker o evitarlos – Editorial Ra-Ma – Año 2007
 - C [CWS01] Robert B. Cialdini, Roselle L. Wissler & Nicholas J. Schweitzer - The Science of influence
 - [KM02] Kevin Mitnik y William Simon – El arte de la intrusión: Cómo ser un hacker o evitarlos – Editorial Ra-Ma – Año 2007
 - [ST01] Sun Tzu, “El arte de la guerra”
<http://www.gabinetedepsicologia.com/downloadclinica/El%20Arte%20de%20la%20Guerra.pdf>
 - [HA01] Hacker Array - <http://hackerarray.mforos.com/>
 - [HA02] El Hacker - <http://www.elhacker.org/>
 - [KM02] Kevin Mitnik y William Simon – El arte de la intrusión: Cómo ser un hacker o evitarlos – Editorial Ra-Ma – Año 2007
 - [KM02] Kevin Mitnik y William Simon – El arte de la intrusión: Cómo ser un hacker o evitarlos – Editorial Ra-Ma – Año 2007
 - [JF01] The jargon File - <http://www.catb.org/~esr/jargon/html/index.html>