



La Ingeniería Social

“Oportunidades que le brindan las nuevas amenazas”

Autor: Maximiliano Visentini, alumno de la
Facultad Regional Córdoba de la UTN
Fecha: Miercoles 13 de diciembre del 2006

Comentario Inicial

Este trabajo forma parte del proyecto de Educación que se organizó conjuntamente con la Universidad Tecnológica Nacional (UTN) de Argentina, donde Maximiliano Visentini fue quien presentó uno de los mejores trabajos evaluados, consiguiendo la publicación del mismo por Eset.

Disclaimer: Ni Eset ni sus partners regionales se hacen responsables de las opiniones y fuentes consultadas por el autor, Maximiliano Visentini, en este documento.

Introducción

Con este trabajo se quiere lograr que una vez finalizado su análisis, el lector tenga en claro el concepto de Ingeniería Social, su objetivo, quiénes lo utilizan, dónde se emplea, quiénes son los más vulnerables y sobre todo, de qué manera las nuevas amenazas como spam, phishing, spyware, etc pueden resultar de gran ayuda para emplear Ingeniería Social.

Para ello, se introducirán algunos conceptos a nivel general de Ingeniería Social, luego se citarán ejemplos de la vida cotidiana. Se describirán en detalle esos conceptos, sus características y sus diferentes aplicaciones y objetivos, pero esta vez a nivel informático. Luego se enumerarán ejemplos (algunos reales y otros no, donde se muestra el efecto producido por determinada causa).

También se verá el rol importante (aunque muchas veces ignorado) del factor humano en cuanto a su concientización y educación sobre la seguridad de los datos que maneja.

Además se describirán los diferentes tipos de ataques a los que el ser humano está expuesto (vía sms, vía correo electrónico, vía telefónica, etc) y debe buscar la forma de estar preparado para evitar estos ataques.

En la siguiente etapa, se tratará sintéticamente al Malware (Software Malicioso) a nivel general, luego se enumerarán y describirán los tipos de malware conocidos (virus, troyanos, spyware, gusanos, etc).

Luego se introducen los conceptos de las nuevas amenazas y qué relación tienen con la Ingeniería Social, quiénes las crean y con qué objetivo.

Conceptos sobre Ingeniería Social

Por ahora, se dirá que la **Ingeniería Social** (Social Engineering) son aquellas conductas y técnicas utilizadas para conseguir información de las personas. Es una disciplina que consiste básicamente en sacarle datos a otra persona sin que esta se de cuenta de que está revelando "información sensible" y que normalmente no lo haría.

A nivel informático, generalmente se usa para conseguir nombres de acceso y contraseñas. Para usar esta disciplina no hay que ser un experto en sistemas, ni requiere muchos conocimientos, simplemente hay que saber a quién dirigir el “ataque” y bastante astucia.

Es un arte... el arte de conseguir algo que nos interesa de otra persona por medio de habilidades sociales (manipulación).

Estas conductas o técnicas que usan estas personas (también llamados Ingenieros Sociales) son tan estudiadas que para alguien que no está embebido en temas de seguridad, son altamente efectivas, y es por eso que la Ingeniería Social es tan preocupante.

Las técnicas utilizadas pueden consistir en mensajes de texto cortos por celulares (SMS), correos electrónicos, llamados telefónicos, cartas, incluso personalmente acreditando credenciales falsas (a veces no es necesario, sólo basta una conversación con mucha convicción haciéndose pasar por otra persona). El objeto de todas estas técnicas, como antes se menciona, es el robar información valiosa sin que la víctima pueda darse cuenta de lo que está revelando, y así utilizar dicha información para su propio beneficio.

La ingeniería social, hoy quizá la técnica más divulgada para propagar algún mal, consiste en la utilización de debilidades en los usuarios, utilizando su desconocimiento o miedo, entre otros factores, para aprovecharse de su ingenuidad.

Si bien el término de Ingeniería Social es bastante novedoso en el ámbito informático, en el mundo cotidiano es tan antiguo como la comunicación misma.

Hoy, nos han manipulado empleando técnicas de Ingeniería Social en algún momento de nuestras vidas sin habernos dado cuenta. La cantidad de ejemplos son incontables.

Estas técnicas consisten en engaños, actuaciones, acciones estudiadas para lograr que otra persona le brinde amablemente acceso a valiosa información u objeto de interés, utilizando una gran astucia y mucha paciencia.

Algunos ejemplos donde se Aplica Ingeniería Social en la vida cotidiana

- Un vendedor que investiga las costumbres y fanatismos de un cliente para poder vender con una mayor facilidad sus productos o servicios.
- La persona en la puerta de una farmacia durante 4 meses con una misma “receta médica” de algún medicamento, pidiendo dinero para poder comprarlo.
- La tarjeta trabada en el cajero automático y que frente a la desesperación del dueño, una persona amable se ofrece a ayudar a recuperarla, hasta finalmente lograr que su víctima digite su código secreto.

Así como estos, son miles los casos en los que nos vemos amenazados a diario por la astucia y mala intención de estos “Ingenieros Sociales”.

La película Argentina “*Nueve Reinas*”, demuestra el típico modelo de cómo se utilizan en la vida real estas habilidades y artimañas para conseguir cosas de otras personas, y muchas veces de manera voluntaria.

Estas acciones están vinculadas con la comunicación entre los seres humanos. Las prácticas realizadas son por lo general engaños, habilidades y trucos para lograr que un usuario (víctima) revele información que comprometa a la seguridad de su empresa.

Las cualidades que tiene que tener el atacante para estas actividades pueden ser varias, como sus relaciones personales, ambición, conocimiento, apariencia de inocencia, credibilidad, curiosidad, etc. No es racional que pidiendo a una persona que nos brinde la información que nos interesa, la obtengamos de manera tan simple; sin embargo, esta habilidad es desarrollada y utilizada por personas normales, hackers, ladrones, y estafadores para lograr que otra persona ejecute una acción que generalmente repercute en un beneficio para el atacante.¹

Desde el punto de vista de la psicología, hay determinados procesos que son automáticos tanto en el ser humano como en los animales en virtud de las relaciones con los demás. Depende de quién

¹ Borghello, Cristian “Ingeniería Social (II)” http://www.segu-info.com.ar/boletin/boletin_060408.htm (2006)

lo analice puede ser una ventaja o una desventaja. Estos procesos son comúnmente utilizados en campañas de marketing y negocios para influenciar sobre la gente.

Una descripción de los procesos básicos de la influencia², sería esta:

- **Reciprocidad** – una persona hace un favor a otra, entonces la otra tiene que devolverle el favor.
- **Compromiso y Consistencia** – una persona dijo que haría una acción y se ve obligada a hacerla, y debe ser consistente con su forma general de pensar.
- **Pruebas Sociales** - es más cómodo hacer lo mismo que hace la gente.
- **Gustarse y ser Parecidos** - le gusta cierta gente, o aquellos que son parecidos a él/ella, y tiende a ser influenciado/a por ellos.
- **Autoridad** – las personas reconocen ciertos tipos de autoridad real o aparente, y los respetan.
- **Escasez** – las personas se sienten atraídas por lo que es escaso.

Ejemplos como Tupperware, Gillette, Coca-Cola, Mc Donald's, y otros grandes del marketing son una clara muestra del alcance de los procesos de la influencia, ya que han logrado introducir en la gente el uso verbal de sus productos como si fueran el molde del producto en si. Alguien se refiere a un “Tupper” cuando en realidad esta refiriéndose a un envase o bol, lo mismo pasa al referirse a una “gillette” cuando en realidad lo que se quiere es una hoja de afeitar. Todo esto, es posible con una adecuada utilización del marketing y procesos de Influencia antes mencionados.

Hasta ahora siempre se habló de la Ingeniería Social en el ámbito de la vida normal o mejor dicho en lo cotidiano. Ahora se comienza a hablar de esta disciplina cuando hay una computadora, una red local, o en presencia de Internet.

Ingeniería Social. ¡Un nuevo ataque a la seguridad Informática!

² Tomado del libro “Influence: The Psychology of Persuasion.” Robert B. Cialdini, Ph.D. (1993).

En materia de seguridad informática, estas técnicas son utilizadas para muchos fines específicos, algunos ejemplos sencillos son:

- El usuario recibe un correo con un título que atrae su atención, o la dirección del destinatario le suena familiar, y esto lo lleva a abrir el archivo adjunto del correo, el cual podría tratarse de un gusano, troyano o algún malware no identificado por su antivirus actualizado, ni por la heurística empleada por el mismo.
- El usuario es llevado a confiar información necesaria para que el atacante realice una acción fraudulenta con los datos obtenidos. Este es el caso del phishing, cuando el usuario entrega información al delincuente creyendo que lo hace a una entidad de confianza (Tema analizado más adelante).³
- El usuario es atraído por un falso anuncio de infección en un sitio web de seguridad informática, donde se aconseja descargar una aplicación antispyware que detecta un supuesto malware, para el que sólo ofrece solución si se compra una licencia.
- Los formularios que un usuario tiene que completar al momento de crear una nueva casilla de correo, con valiosa información tales como ingresos anuales promedio, gustos y hobby, edad y otros datos personales con los que fácilmente luego pueden hacerles “ofertas a medida”.
- La voz agradable de una mujer o en caso contrario la voz de un hombre, que pertenece al soporte técnico de la empresa del usuario, que le solicita telefónicamente información para resolver un inconveniente detectado en la red.
- El llamado de un usuario al Administrador del Sistemas que necesita que le blanqueen su clave, porque la cambió durante el transcurso del día y no la recuerda. A simple vista esto no parece algo fuera de lo común, pero si el llamado propiamente dicho no es efectuado por el usuario quien dice ser, sino por un Ingeniero Social, la información personal sería entregada al atacante por el mismo Administrador del Sistema. Con esta astucia y un Administrador desprevenido o desinformado, este método es completamente viable.

Objetivos de la Ingeniería Social

Estos pueden ser varios. Entre ellos:

³ Tomado de un Artículo por Borghello, Cristian http://www.segu-info.com.ar/boletin/boletin_060408.htm

- Conseguir beneficios económicos para los creadores de malware y estafadores debido al ínfimo costo de implementación y el alto beneficio obtenido.
- Realizar compras telefónicamente o por Internet con medios de terceros, conociendo bastante sobre ellos (datos personales, tarjeta de crédito, dirección, etc).
- Acceder gratuitamente a Internet si lo que se buscaba era nombre de usuario y contraseña de algún cliente que abone algún servicio de Banda Ancha.

Un Ejemplo Verídico

Aún las más grandes empresas que invierten millones de dólares al año en la seguridad de sus datos, fueron víctimas de estos ataques de Ingeniería Social.

De una forma más específica, un excelente ejemplo donde se muestra la imaginación de los “Ingenieros Sociales”, es la auditoria a la que fue sometida en junio de este año, una empresa estadounidense que se dedica a conceder créditos, siendo el objetivo el de mostrar la inseguridad de las memorias USB.

La empresa tomó 20 memorias USB de muestra, les pusieron archivos de varios tipos, incluyendo un troyano que una vez ejecutado en cualquier computadora comenzaría a enviar información a los servidores de la empresa auditora, y los fueron dejando «olvidados» en el estacionamiento, zonas de fumadores y otros sitios de la empresa bajo auditoria.

De las veinte memorias, quince fueron encontradas por empleados de la empresa en cuestión, y las quince terminaron por ser enchufadas en computadoras conectados a la red de la compañía, que en seguida empezaron a enviar datos a la empresa Auditora que les permitieron entrar en sus sistemas sin ningún problema.⁴

Con todo esto, es fácil deducir que aún con la mejor tecnología, los mejores profesionales a cargo de los datos de su empresa, no hay forma alguna de protegerse contra la Ingeniería Social, ya que tampoco hay usuarios ni expertos a salvo de estos ataques. La Ingeniería Social, siempre existió, nunca pasa de moda, día a día se perfecciona, no va a morir nunca, y tiene un limite.... la Imaginación Humana.

“La Seguridad muchas veces es una mera Ilusión. Una compañía puede tener la mejor tecnología, firewalls, sistemas de detección de intrusos, dispositivos de autenticación avanzados como tarjetas biométricas, etc y creen que están asegurados 100%. Viven una Ilusión. Sólo se necesita un llamado telefónico y listo. Ya son vulnerables a un ataque. La Seguridad no es un producto, es un Proceso”⁵

Uno de los hackers / phreakers (dependiendo de quién lo use al término) más importantes de las últimas décadas que utilizó Ingeniería Social es **Kevin Mitnik**. Quien por su ambición de querer conocer cuanta tecnología se inventara, y buscarle hasta la más mínima falla a la misma, realizó

⁴ Nota original en http://www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1

⁵ Mitnik, Kevin. “The Art of Deception” E-book, paginas 12, 13 (Traducción Propia)

crímenes informáticos y actos ilícitos, que le dieron un pase libre hacia la cárcel en la que pasó ocho años. Desde el 2002 está libre, con derecho de utilizar una computadora, Internet, teléfonos celulares y tiene su propia empresa incluso, en la que trabaja como consultor en temas de seguridad, especialmente Ingeniería Social. También colabora con la sociedad escribiendo sus experiencias y conocimientos. Ya tiene varios libros publicados sobre seguridad informática.

Hay una única “salvación” y es la **Educación**. En realidad es una forma efectiva de estar protegido contra la Ingeniería Social.

La gente por no querer quedar mal o armar un escándalo, brinda a cualquiera que le solicita, “información sensible”, y ahí es donde juega un papel importante la educación, el enseñarle a los empleados a decir no.

En este caso no se trata de una educación estrictamente técnica, sino más bien una capacitación social que alerte a la persona cuando está por ser blanco de este tipo de ataque. Si el Ingeniero Social tiene la experiencia suficiente, puede engañar fácilmente a un usuario en beneficio propio, pero si este usuario conoce estas tretas no podrá ser engañado. Además, la educación de los usuarios suele ser una importante técnica de disuasión.

Con todo lo dicho hasta ahora hay una conclusión que salta a los ojos de cualquier lector, y es que el ser humano es el eslabón más débil de cualquier sistema. Los encargados del mismo pueden haber tenido en cuenta hasta los más ínfimos detalles en el armado de la red (hablando en materia de seguridad informática) y aún así siempre es un usuario quien está frente a una computadora, tomando decisiones y haciendo uso del sistema. Los diseñadores pueden haber tenido en cuenta todos los patrones de seguridad al momento de diseñar el sistema y aún así será siempre un humano quien manipule en algún momento los datos.

Por ende, es el ser humano el objetivo y el medio para acceder al sistema, entonces es de alta importancia la capacitación para cada usuario con acceso al sistema, y que internalicen que todos somos un eslabón más en la cadena de la seguridad de los datos de la empresa.

¡Conociendo a la Víctima!

Sólo basta recolectar una buena cantidad de información del individuo (víctima) tales como sus hábitos, nombres de familiares, esposo/a, fechas importantes, etc. y la persuasión viene casi garantizada. El atacante utilizará la información conseguida para sonar convincente, o hacerse pasar por otra persona (familiar, empleado de la misma empresa, etc) consiguiendo así un fácil acceso a lo que realmente busca.

Para la recolección de información hay muchas técnicas conocidas⁶, entre ellas:

- Telefónicamente, el atacante se hace pasar por otra persona o sorprende en su buena fe al usuario aprovechándose de su ignorancia o inocencia, y así consigue información importante.
- Investigando en los contenedores de basura de la víctima. Pueden encontrarse datos útiles como horarios de vigilancia, nombres y códigos de empleados, procedimientos de la empresa, códigos fuente, discos u otros dispositivos de almacenamiento, etc.
- Por Internet (consiguiendo que el usuario se loguee en algún sitio, soft de mensajería, etc) obteniendo dicha clave. Con un poco de suerte el usuario utiliza esa misma contraseña y nombre de usuario para cualquier situación (al ingresar al sistema de su trabajo, PayPal, Ebay, Banco, etc)
- Mirando por encima de los hombros de alguien mientras escribe su nombre de usuario o contraseña privada.

Por supuesto, se va a tender a elegir una víctima débil. Se va a comenzar desde el que tenga menos conocimientos hacia el que mas posea, ya que los argumentos tienen que ser contruidos generando una situación creíble para que el individuo realice la acción que se desea.

Un Ejemplo Increíble, pero “REAL”

A fines de mayo del 2004, en la Boda Real (Felipe y Leticia) donde se procedió a un operativo de Seguridad⁷ que costó entre seis y ocho millones de euros, incluía veinte mil agentes, doscientos francotiradores, sellado de alcantarillas, corte de todo el centro de la ciudad durante dos días (calles, metro, autobuses), vigilancia casa-por-casa de todo el recorrido durante meses, cierre del espacio aéreo sobre Madrid, dos aviones cazas F-18 volando durante la boda y otros dos aviones AWACS prestados por la OTAN; El famoso coronel ya retirado Amadeo Martínez Inglés⁸ logró infiltrarse en la Catedral en plena Boda con un arma en la cintura y su traje de militar burlando seis controles de seguridad con sólo saludar amablemente a los oficiales y sin poseer ninguna

⁶ Bearman, Ross (Sir Ross). “A Guide To Social Engineering – Vol.1” (2004) (Traducción Propia)

⁷ Nota completa del operativo en: http://www.cadenaser.com/articulo.html?xref=20040521csrscsnac_12&type=Tes

⁸ Coronel del Estado Mayor y escritor, dado de baja del servicio activo por una falta de disciplina y encarcelado 5 meses en la prisión militar de Alcalá de Henares por cuestionar en 1990, el servicio militar obligatorio y proponer públicamente la creación de un Ejército profesional.

credencial o invitación para ello. Esto fue una excelente demostración de un grave fallo de los servicios de Seguridad de la Casa Real, teniendo en cuenta que sólo le tomo ocho minutos atravesar seis controles de seguridad a lo largo del recorrido.⁹

⁹ Nota del Hackeo Social en: <http://www.elmundo.es/elmundo/2004/05/24/espana/1085401631.html>

Formas de Ataque

Las formas de ataque son muy variadas, y dependen única y exclusivamente del ingenio del atacante, pero las más comunes hoy son utilizando el teléfono, vía e-mail, incluso el mismo correo postal, los celulares a través de mensajes de texto cortos (sms) y los ataques personales valiéndose de la ingenuidad de la gente o la falta de capacitación.

Ataques Telefónicos

Es uno de los más eficientes, debido a que las expresiones del rostro no son reveladas y el atacante puede utilizar todo su potencial de persuasión.

A continuación se cita un claro ejemplo¹⁰ de su funcionamiento:

Janie Acton llevaba trabajando más de tres años para una empresa en Washington, D.C., como representante de servicios al cliente. Era considerada una de las mejores en su rubro. Todo iba bastante bien cuando esta llamada tomó curso. Desde el otro lado del teléfono se oyó:

“Soy Eduardo del Sector de Facturación. Tengo a una mujer esperando en el teléfono, me está preguntando por cierta información y no puedo utilizar mi computadora por que al parecer está infectada con algún virus. De cualquier forma,

¿Podrías buscar cierta información de clientes para mí por favor?

J- “Por supuesto” contestó Janie.

J- “¿En que te puedo ayudar?” Preguntó Janie

Aquí el atacante buscó información que había recopilado con su investigación para sonar creíble y auténtico. Aprendió que la información que buscaba estaba almacenada en algo llamado “Sistema de Información sobre Facturación de Clientes”, y también se dio cuenta como los empleados se referían al sistema. Entonces él preguntó:

¹⁰ Mitnik, Kevin. “The Art of Deception” E-book, paginas 40, 41 (Traducción Propia)

E- “¿Me podrías buscar una cuenta del SIFC?”

J- “Sí claro, ¿cuál es el número de cuenta?”

E- “No tengo el número; Necesito que lo busques por el nombre del cliente.”

J- “Bueno, ¿Cuál es el nombre entonces?”

E- “Es Heather Marning.” Deletreó el nombre, y Janie lo escribió...

J- “Perfecto, aquí lo tengo.”

E- “Genial. ¿La cuenta sigue vigente?”

J- “Sí, está vigente.”

E-“¿Cuál es el número de cuenta, dirección y teléfono?”

J- "Número de Cuenta BAZ6573NR27Q." y así Janie le suministró el resto de los datos que el atacante había solicitado.

Ataques Vía Web

Hoy, sólo hacen falta pocas cosas para causar pánico, una conexión a Internet y malas intenciones.

Es en este tipo de ataque, cuando el Ingeniero Social juega con la desinformación y sentimientos de las personas, ya que pone en marcha un plan estratégico, que sólo los análisis estadísticos pueden mostrar la eficiencia y eficacia que obtienen al realizarlos.

No se trata de otra cosa que un simple correo electrónico del cual no se sospecha y puede venir disfrazado de muchas formas, ya sea que la dirección de correo electrónico resulte familiar o el asunto del e-mail de cierta forma “ataque” los sentimientos como la curiosidad, la avaricia, el sexo, la compasión o el miedo y es donde el usuario se vuelve susceptible a abrirlo... ¡ERROR! Fue la peor decisión que se podría haber tomado, pero por otro lado la que en ese momento predominó.

En este punto, podrían aplicarse varias estrategias como medios de ataque, estas son algunas:

1. Se trata de algún código malicioso en un archivo adjunto (virus, troyano, etc) de un e-mail que algún conocido ha enviado.
2. Una cadena reenviada (muchos usuarios no piensan que es malo), pero tampoco es cierto nada de lo ahí descrito. Ni Hotmail va a cerrar, ni la persona que amas va a llamarte si envías ese correo a mil amigos, mucho menos Microsoft va a donar a niños de África U\$S 1.00 por cada e-mail que envíes. Sólo logran que pierdas tiempo, crear bases de datos de correos electrónicos para luego venderlas a empresas que te llenaran la casilla de “basura”, conocidos como Hoax.
3. Un mail confirmando una compra (falsa) de cierta mercancía con tu tarjeta de crédito, agradeciendo al cliente y dejando un número de teléfono en caso de alguna duda o queja del servicio. El número al que se llama no pertenece a ninguna compañía, sino que es una especie de 0-609 donde te atiende una grabación solicitando espere unos instantes, ya que los representantes están ocupados. En eso consiste el robo, la víctima por el pánico de una compra que nunca realizó, efectiviza dicha llamada donde le cobran entre \$1 y \$4 por cada minuto que está conectado. ¡Nunca nadie lo atenderá en realidad!
4. Un mail de alguna empresa de manejo de dinero (Algún Banco, Pay-Pal, Western Union, etc.) en la que estés suscripto donde te ofrecen algún beneficio y que para acceder al premio tienes que loguearte y controlar tus datos personales. Por supuesto, al hacer clic sobre el link te estarás direccionando a una pagina del “atacante” idéntica a la que tu conoces, pero hosteada en un servidor gratuito, tus datos serán guardados a una tabla para luego utilizar tu cuenta en “enormes compras”, y te aparecerá un mensaje de error que te redireccionará a la pagina legítima de la empresa y no te darás cuenta hasta que llegue el resumen de tu tarjeta de crédito por lo menos. Esta técnica es conocida como phishing.
5. Una llamada telefónica o mensaje de texto (SMS) de un banco, informando que han cerrado o suspendido tu cuenta por falta de pago o cualquier excusa, no es otra cosa que vishing (phishing a través del teléfono) y esta vez lo hacen utilizando voz sobre IP (VoIP), telefonía móvil y telefonía terrestre.

Para hacerlo mas claro, se plantea un ejemplo a continuación:



Ataques Vía Correo Postal

De esta manera se obtiene de forma precisa datos de la persona a quien se desea atacar.

En Estados Unidos uno puede contratar una casilla postal donde se recibe y desde donde se envía toda la correspondencia.

Se toma como patrón a alguna suscripción de revista o cupones de descuento de la zona donde vive la víctima e imita los formularios correspondientes (lo más similar posible) modificando sólo la dirección original por la reciente creada casilla de correo. Se crea una propuesta muy atractiva para al menos detonar curiosidad en la víctima. El atacante solicita una clave en el formulario donde aclara que esta le servirá para reclamar su premio (ya que esta comprobado que el usuario promedio utiliza la misma clave para múltiples usos)

En el siguiente paso, la víctima completará los formularios y los enviará a la casilla de correo del atacante. Teniendo este último, los datos de la víctima, ya está en condiciones de llevar a cabo el verdadero ataque.

Ataques Vía SMS

Estos son, quizá los más novedosos por que la gente piensa que está más protegida, piensa que es un medio de alta seguridad, y es por eso que los hace más vulnerables, los ataques son muy parecidos a los de otros medios. Por lo general, felicitando por haber ganado mensajes de texto (sms) gratis de tu empresa prestadora de teléfono, o haberte ganado algún premio en un sorteo o alguien que te enseña como hacer para que tu línea tenga más crédito. Con sólo mandar un simple mensaje obtendrás este regalo.

No se trata de ningún regalo en absoluto, sino que estás transfiriendo parte del saldo de tu línea a la persona que te envió el mensaje. Es un servicio que brindan las compañías de telefonía celular a sus clientes para transferir crédito a otra persona.

Para verlo más claro, aquí va un ejemplo:



En este mensaje, se está enviando al celular con característica de Buenos Aires (011) y número 15x-xxxxx52 la suma de \$18. Los cuales serán restados del saldo de quien envía el mensaje por la codicia de recibir crédito gratis.

Ataques Cara a Cara

Estos son los mas eficientes, pero los mas difíciles de realizar, la víctima ha de ser alguien con un alto nivel de desinformación y de conocimientos, también son susceptibles aquellos en los que su mente no está preparada para tal maldad (ancianos, niños, personas insanas).

Haciéndolo más real, se plantean algunos ejemplos:

Caso 1:

Hoy los sistemas de cobro se han automatizado en un 99% se podría decir. Salvo excepciones, todos utilizan los cajeros automáticos para recibir sus haberes mes a mes. Imagine que un anciano de ochenta años que como todos los meses, se dirige a su banco para cobrar su jubilación, pensión o aguinaldo, y le informan que de ahora en más, sus cobros se realizan por medio del cajero automático. Esa persona frente a una computadora que le da instrucciones y con un límite de tiempo para realizar dicha tarea probablemente no le resulte fácil, quizá nunca aprenda a manejar un cajero automático y sea víctima de alguien que se presente a “ayudarlo”, o a “enseñarle” como manejar la computadora.

Caso 2:

Los niños son muy susceptibles a aceptar casi cualquier cosa que un adulto le diga como verdad y por el mismo camino responden ante cualquier pregunta que un extraño le pueda hacer. Imagine a un chico en la escuela, que confía en sus maestros, la potencial víctima que es al contestar preguntas referentes a sus padres (horarios de trabajo, posición económica, orientaciones religiosas, políticas, lugar dónde guardan su dinero, etc) Si bien esas preguntas son muy puntuales, si el chico conoce las respuestas y quien se lo pregunta le inspira confianza, es muy probable que el chico le otorgue esa valiosa información.

Por otro lado es muy fácil ganarse la confianza de un niño. Todo el mundo conoce por ejemplo la debilidad de ellos por las golosinas y los juegos.

Caso 3:

Una persona insana puede poseer información valiosa, ya sea almacenada en su cabeza como en otro sitio, y tras un trabajo de persuasión adecuada podría llegar a revelarla a un desconocido, debido a que probablemente no se encuentre en un estado conciente de sus actos.

Caso 4:

Una persona que trabaja como secretaria/o de una empresa maneja y dispone de información sensible, pero que quizá desconozca tal importancia, entonces se le presenta un Ingeniero Social haciéndose pasar por alguien que trabaja dentro del área de cómputos de la empresa, y le solicita su nombre de usuario y contraseña para realizar un control rutinario de seguridad, al que otros empleados colaboraron. Y con amabilidad y firmeza logra obtener la confianza del empleado/a obteniendo la información deseada.

INTRODUCCION AL MALWARE

El Malware (termino formado a partir de combinar las palabras Software Malicioso) es un programa diseñado para hacer algún daño a un sistema. Puede presentarse en forma de virus, gusanos, caballos de Troya, etc, y se ejecuta automáticamente sin consentimiento ni conocimiento por parte de la víctima.

Este malware puede parecer totalmente indefenso, incluso presentarse como un archivo .doc o .xls o cualquier otro programa que tenga funcionalidad de macros, por ejemplo.¹¹

Unos de los más difundidos son los virus y gusanos, no por eso hay que despreocuparse del resto (rootkits, troyanos, spyware, exploits). Los virus y gusanos tienen como semejanza la capacidad de que se auto-repican y pueden (en efecto lo hacen) copiarse e infectar una red completa. Sin embargo, la diferencia consiste en que el virus necesita un portador para replicarse, o sea algún archivo en el que incluirse, en cambio los gusanos no necesitan de un portador.

Los portadores más comunes que utilizan los virus son varios, entre ellos los archivos ejecutables que incorporan las aplicaciones, los antiguos discos de 3 ¼ (en el sector de booteo), las memorias usb, y los archivos que contengan macros. En el caso de los archivos ejecutables, cuando el usuario corre la aplicación se ejecuta el código del virus, y por lo general la aplicación portadora funciona correctamente.

Los gusanos (worms) son muy parecidos a los virus, pero estos no dependen de un archivo portador para funcionar. Muchas veces se basan en las flaquezas del objetivo o utilizan Ingeniería Social para lograr que los ejecuten los usuarios.

Un Troyano (Trojan Horse) es un programa dañino, utilizado normalmente como herramienta para espiar, que suele presentarse disfrazado de otro programa o como pequeña parte de un archivo que parece indefenso como ser un archivo multimedia, un documento, una planilla de cálculo, etc. Estos no tienen la capacidad de auto-replicarse, pero pueden ser adheridos a cualquier tipo de software. El problema muchas veces es que a la vista del usuario el archivo o programa funciona correctamente, el problema está en lo que no se ve. Lo que ocurre a escondidas del usuario.

Por ejemplo, un archivo adjunto recibido en un correo que dicen ser ofertas de un comercio de la zona especializado en electrónicos. Al abrir la imagen que contiene las ofertas, este es abierto correctamente y efectivamente muestra las ofertas pero a su vez se ejecuta un programa que el usuario no conoce, el cual busca información almacenada en la computadora, como ser números y claves de tarjetas de crédito.

Un spyware es un software que tras recopilar información de usuarios la envía al servidor de la empresa a la cual le interesa conocer información de usuarios. Muy utilizado para que las corporaciones conozcan los hábitos de las personas, como ser las páginas que visitan, la información que buscan, el tipo de productos que le interesa comprar por Internet, etc. Con ello podrán luego ofrecerles publicidades a medida o vender esa información a otras empresas.

¹¹ Mitnik, Kevin. “The Art of Deception” E-book, paginas 91 (Traducción Propia)

Un keylogger es un programa malicioso que registra cada vez que se pulsa una tecla en el teclado y se almacenan en un archivo de texto. Estos programas están pensados para robar información privada de una persona, como por ejemplo números de identificación personal (DNI, CI, LC, LE), nombres de usuarios y contraseñas, números de tarjetas de crédito con sus respectivas claves o PIN.

Estos pueden ser detectados por un antivirus actualizado, algún anti-spyware o en el mejor de los casos un anti-keylogger.

Para el usuario que no posee una computadora aún, y tiene que hacer uso de las mismas en un cybercafé (usuario nómada) es un problema de gran preocupación, debido a que estos poseen un escaso mecanismo de seguridad (muchos no tienen un antivirus instalado en sus PCs siquiera)

Esto resulta una gran amenaza a la privacidad de los usuarios, y más aún, una amenaza hacia la sociedad por un problema tan elemental como la carencia de educación y respeto hacia el resto.

Un exploit es un software que aprovecha alguna debilidad de un sistema operativo. Los exploits no necesariamente son maliciosos. Generalmente los crean expertos para demostrar que existe un fallo en la seguridad del sistema.

Un rootkit, es un programa que utiliza un atacante luego de andar ilegalmente por un sistema, para ocultar su presencia y a su vez dejarle garantizado el ingreso nuevamente en un futuro. Por otro lado también permiten esconder procesos activos, archivos en uso y modificaciones al sistema.

LAS NUEVAS AMENAZAS

“Herramientas que brindan ayuda a la Ingeniería Social”

Quiénes y con qué objetivo las crean

Hay diferentes “herramientas y técnicas” que se crearon no hace mucho y se siguen creando por Ingenieros Sociales, programadores de malware, estafadores, etc. Algunos con el fin de atraer usuarios a determinadas paginas donde se les ofrece algún producto lícitamente, otros con el fin de llevarlos engañados a una página web “idéntica” a la de algún banco, o entidad que permita hacer pagos por Internet como PayPal, donde se le solicita al usuario el ingreso de sus datos

personales para luego utilizarlos de manera ilegal. Otros recopilan información del usuario sin que este se de cuenta, etc.

Estas herramientas son algunas de las nuevas amenazas que hoy están “disponibles”. Estas no siempre van a ser malas, puede haber ocasiones en los que exista una herramienta que sirva para recopilar información de sospechosos o delincuentes.

Algunas Herramientas:

Phishing

El phishing es un engaño tan dañino y eficaz como se pueda imaginar, utilizado siempre para fines delictivos. Básicamente consiste en algún e-mail que procede al parecer de un negocio o empresa legítima y digna de confianza (un banco o compañía de crédito) solicitando “verificación” de los datos y advirtiendo sobre consecuencias que traerían si no se hiciera dicha verificación.

El mensaje y/o notificación por lo general tiene un enlace que conduce a un sitio web fraudulento que a simple vista es idéntico al legítimo, incluso con todos los logotipos propios de la empresa, contenido imágenes, y un formulario que solicita muchos datos (que van desde la dirección hasta la contraseña de acceso de la tarjeta de crédito o débito) que una vez ingresados estos datos por el usuario, van directo a las manos del falsificador.

El phishing tiene como gran aliado al spam, ya que este e-mail fraudulento se envía indiscriminadamente a miles de usuarios tomados de bases de datos, donde siempre alguno (un poco crédulo) ingresará sus datos en esta falsa página web y probablemente los daños que sufrirá serán de un alto impacto. Podría perder todo el dinero de su cuenta bancaria o tarjeta de crédito.

Spyware

El spyware (software espía) recopila información desde una computadora sin el conocimiento y consentimiento del usuario (ya sea particular o en una empresa). Busca información especial del usuario o la empresa para conocer las actividades que se realizan en Internet (no es su peor utilización, pero sigue siendo invasión a la privacidad) para luego generar estadísticas. También con el mismo método se puede usar dicha información para vendérsela a empresas y poder así ofrecer al usuario productos a medida.

Por otro lado, están los más perjudiciales que capturan, guardan y envían al atacante todo lo que se ingresa desde el teclado. Incluso los más avanzados pueden hasta vigilar a un usuario con su propia web-cam o micrófono, sin que el mismo usuario sepa que estos dispositivos se encuentran activados.

Estos pueden ser instalados en una computadora personalmente, o mediante un virus o un troyano que se distribuye a través del correo electrónico.

Spam

Spam se dice ser el envío masivo y no solicitado de e-mails, normalmente con contenido publicitario de productos o servicios dudosos, métodos para hacerse ricos o adelgazar rápidamente. Si una persona recibe un mail que no solicitó de alguien que no conoce, y que al mismo tiempo es enviada a muchas personas que tampoco lo solicitaron; eso es spam.

Esta actividad es muy perjudicial, debido a que está causando una molestia al usuario, sin mencionar el costo de tiempo y dinero que pierde en esa lectura (ya que muchos usuarios aun tienen una conexión a Internet en la que pagan según al tiempo que esté conectada).

Características más comunes del Spam

- El remitente del mensaje (reply) suele ser una dirección inexistente o ficticia.
- La dirección que ahí figura puede parecer muchas veces la del algún conocido, pero leyéndola con atención podrá evidenciarse una leve diferencia, lo que dificulta aún mas para el usuario común no abrir dicho correo.
- El asunto del mensaje suele ser muy llamativo
- El contenido es publicitario en su mayoría (ofertas de comercios, métodos para recibir grandes cantidades de dinero en poco tiempo, sitios para hacer amigos/as online), pero también para distribuir malware y amenazas como phishing, spyware, etc.

Otros nombres de Spam dependiendo su forma de distribución

Si bien se conoce al Spam por medio del correo electrónico, no es su única ruta de distribución. Este fue evolucionando, desde los correos electrónicos, pasando por los programas de mensajería instantánea hasta los celulares y las conversaciones telefónicas por IP. Cada cual tiene su nombre y estos son:

- Spam: enviado a través del correo electrónico.
- Spim: Spam sobre mensajería instantánea (MSN Messenger, ICQ, etc).
- Spam SMS: Spam que se difunde por dispositivos celulares mediante la tecnología SMS (mensajes de texto cortos).
- Spit: Spam sobre telefonía IP también conocida como VoIP (Voice over Internet Protocol, es la tecnología que permite realizar llamadas telefónicas a un muy bajo costo ya que envía la voz en forma de datos a direcciones en Internet en vez de hacerlo a un teléfono fijo).

Cuando alguien recibe un correo spam por lo general tiene una opción de ser removido de la lista (para no recibir más ese correo) con sólo enviar un e-mail solicitando que lo borren de dichas listas. Haciendo eso, el usuario no sólo que no conseguirá ser borrado de las listas, sino que estará confirmando que su dirección de correo efectivamente existe y comenzará a recibir más mensajes spam aún.

Por lo general, las direcciones son robadas, compradas, recolectadas de la web y/o tomadas de cadenas de mails.

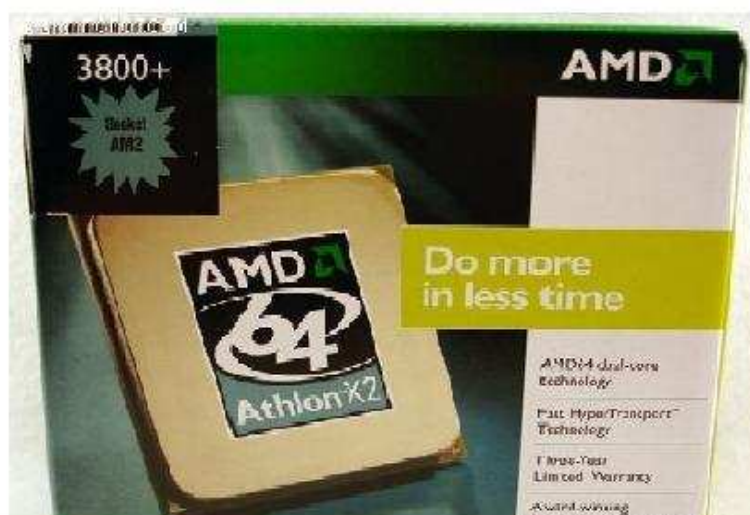
El spam está siendo utilizado como instrumento para elevar el valor de acciones de bolsa de forma puntual.

Muchos de estos spammers hacen alusión a una supuesta ley que dice que el mensaje que están enviando no es spam si posee una forma de ser eliminado.

Hacen referencia al decreto S.1618 Título III, el cual no existe hasta la fecha en Argentina.

Este es un real y claro ejemplo de cómo funciona:

U\$S 33,00 POR 10 UNIDADES MICRO AMD ATHLON 3800 X2 DUAL CORE S AM2/940



Bajo el Decreto S.1618 TITULO III aprobado por el 105 Congreso este mail no puede ser considerado SPAM mientras incluya la forma de ser removido. Para ser removido de futuros correos simplemente envíe un mail a www_banking@webpromotions.com.ar con "Borrar" en el Asunto y será eliminado de esta lista no recibiendo nuevos mails.

En Argentina, los delitos informáticos están a un paso de ser incorporados al código penal, por cuanto los diputados de distintos partidos unificaron los doce proyectos presentados sobre el tema. Las posibles sanciones van de un mes hasta un máximo de seis años de **prisión para quien facilite para su difusión datos electrónicos obtenidos indebidamente**. También contemplaría multas entre \$10.000 y \$100.000.¹²

En la actualidad ya existe un proyecto de ley, que protege la privacidad de las personas en el marco informático, y es el 5864-D-2006 titulado "Código Penal. Modificaciones sobre Delitos

¹² Clarín, BsAs 11 de Octubre de 2006, Página 40, "Delitos Informáticos: Lo trataría hoy diputados"

contra la integridad sexual y la privacidad" que fue aprobado el 11 de Octubre de 2006. Este ya cuenta con media sanción y espera su tratamiento para pasar luego al senado.¹³

Una cifra obtenida de Internet, estima que el 70% de los mails internacionales que se enviaron en invierno de 2006 fueron spam.¹⁴

¹³ Nota en <http://www.vialibre.org.ar/?p=3748>

¹⁴ Nota en <http://www.miguelvillanueva.com/2006/09/16/nuevo-estudio-sobre-el-spam>

Algunos Ejemplos

- En el mes de Septiembre de 2005, un engaño muy ingenioso, fue el de un sitio web relacionado con la Seguridad Informática (al que se accedía mediante una mail **spam** u otros medios) donde se informaba que la computadora estaba infectada con alguna especie de virus nuevo y a su vez redirigía al usuario a una página que simulaba el sitio de Windows Security Center de Microsoft y aconsejaba descargar una aplicación Anti-Spyware que detecta un hipotético **malware**, para el que sólo ofrecía solución comprando la licencia del mismo. Si el usuario elegía la opción aceptar (aceptaba que tenía un malware y accedía a descargar la aplicación) este era dirigido a un sitio donde descargaba la aplicación SpyTrooper que detectaba un falso Malware y solicitaba que se registre para eliminar el spyware (donde tenía que pagar por ello).¹⁵
- En enero de 2005, luego de producido el tsunami, aparecieron delincuentes que se aprovecharon del maremoto, y enviaron e-mails para sacar provecho de la ola de donaciones, esta vez haciendo uso del **phishing**. Hicieron campañas de **spam**, para atrapar a los ingenuos. Como siempre en estos casos se ofrecen enlaces para que el usuario desprevenido haga clic y se conecte a páginas web sospechosas y “realice su donación”.¹⁶
- El 9 de octubre de 2006, otro **troyano** se propaga por Internet y atrae a usuarios a las páginas infectadas mediante un mensaje masivo en forma de spam utilizando eficientes técnicas de Ingeniería Social, donde se informa de un supuesto robo millonario en el Reino Unido por el que ofrecen una recompensa millonaria a cualquiera que aporte un dato relevante para encerrar a los delincuentes. El usuario es invitado a ver imágenes de los delincuentes y de esa manera tratar de reconocer alguno, y así el usuario es redirigido a diferentes sitios (hasta llevar a uno donde efectivamente hay noticias, pero sobre problemas de EEUU e IRAN, aunque en ningún momento hace mención a tal recompensa). En cambio, el usuario decide cerrar el navegador y ya es tarde para entonces, se ejecuta un iframe (Inline Frame) oculto que llama al sitio web <http://www.inthost7.com/counter.php>. Este archivo counter.php va direccionando de un archivo a otro según el navegador que tenga el usuario como así también el Sistema Operativo que utilice.¹⁷

¹⁵ Nota en <http://www.pergaminovirtual.com.ar/revista/cgi-bin/hoy/archivos/2005/00000605.shtml>

¹⁶ Nota en <http://www.virusprot.com/Teletipo501.html>

¹⁷ Nota en <http://seguinfo.blogspot.com/2006/10/troyano-propagandose-en-las-ultimas.html>

Conclusión

Resumiendo todo lo visto hasta ahora, se puede inferir que los programadores de amenazas han elegido la Ingeniería Social como técnica de infección principal. Valiéndose de la inocencia de las personas, consiguen sembrar caos por todas partes.

Si bien es de vital importancia la correcta conservación y cuidado de los datos de una empresa, dentro de ella debe considerarse como factor muy importante al hombre, que es el eslabón más débil en la cadena de seguridad.

Es increíble que estas cosas sucedan hoy... que nos hemos dedicado con tanto énfasis a avanzar en la tecnología, y no podamos resolver este eslabón previo: ¡la debilidad del ser humano! Primero habría que capacitar a quienes estén frente a cualquier sistema o dispositivo electrónico tanto para poder operarlo como para que valore que la información que ahí se almacena o gestiona, es de vital importancia para la empresa. Claro está que no somos máquinas, somos seres racionales, y con muchos sentimientos, y es ahí justamente donde hay que poner **énfasis**, en preparar al personal de manera que NO REVELEN ninguna información a nadie por mas que sientan la necesidad de ayudar. Esta gente (Ingenieros Sociales) son capaces de cualquier cosa, y van a usar lo que este a su alcance para hacerles creer algo que no es, como hacerse pasar por personal de sistemas, o un empleado que perdió su clave y necesita que sea reestablecida, etc.

“La verdad es que no hay tecnología en el mundo capaz de prevenir un ataque de Ingeniería Social”¹⁸

Hoy, según análisis revelados¹⁹ por un estudio sobre amenazas de seguridad de la información, se infiere que de 574 organizaciones encuestadas, el 59% de ellas indicó que su última grieta de seguridad fue por un error humano.

Existen un sinnúmero de consejos para disminuir estas amenazas. Va a depender de las necesidades y lo que este dispuesta a invertir una empresa en seguridad. Algunos son:

- A la hora de contratar un nuevo empleado, buscar preferentemente el que tenga conocimientos de seguridad informática, o en su defecto invertir para capacitar y concientizar al mismo.

¹⁸ Mitnik, Kevin. “The Art of Deception” E-book, pagina 232 (Traducción Propia)

¹⁹ Análisis realizados por la Empresa CompTIA (Computing Technology Industry Association)

- Asegurarse de concientizar y capacitar también a los empleados antiguos sobre las nuevas amenazas, los métodos de acceso inseguros a sus computadoras, y también por supuesto en políticas y procedimientos de seguridad.
- Lograr que los empleados asimilen de que manera son susceptibles ante los métodos de engaño de los Ingenieros Sociales y mostrarles con ejemplos reales (cuya repercusión haya sido muy grande) de manera que logren medir el peligro de brindar cualquier información a un extraño. De esta manera estarán mucho mas preparados ante cualquier intento de manipulación.
- Usar la tecnología apropiada de seguridad y combinarla con políticas bien definidas sobre pautas de comportamiento de los empleados. Algunas políticas pueden ser:
 - No ejecutar ningún programa sin conocer su origen y sin previa autorización de un superior
 - No informar a nadie por teléfono o correo electrónico, sobre características de la red, ubicación de las mismas, datos del encargado de la red, etc. Antes corroborar que esa persona es realmente quién dice ser.
 - No tirar información técnica a la basura, sino utilizar los trituradores de papel correspondientes o destruirlos con cualquier medio.
 - No crear contraseñas fáciles de intuir conociendo a la víctima. Ej.: nombre de la esposa o hijos, número de DNI, fechas importantes, etc. Sino contraseñas combinadas alfanuméricamente, incluso con caracteres especiales. Y a su vez acostumbrarlos a modificar dicha clave periódicamente.

Es de esperar que en poco tiempo contemos con la legislación que respalden y protejan las medidas de seguridad informática antes sugeridas y que garanticen la confidencialidad de los datos. La aplicación de las sanciones desalentaría a jóvenes deseosos de demostrar su supuesta habilidad y conocimientos técnicos.

Propuesta

Como estudiante de Ingeniería en Sistemas de la UTN - FRC, y conociendo en detalle el plan de estudios de la carrera, y también la situación actual por la que atraviesa el país y las empresas, me gustaría que la propuesta de cambio surgiera desde sus raíces, o sea los futuros líderes empresariales y de entidades gubernamentales. Si se planificara un proyecto de educación y concientización para líderes (Ingenieros, Contadores, Licenciados en Administración de Empresas, Licenciados en Recursos Humanos, Abogados, etc) cuando llegue la hora de controlar o gestionar estas entidades, sabrían lo valioso que es el cuidado de la información y pretenderían el mismo cuidado por parte de cada empleado.

Si bien no es óptima la situación que atravesamos actualmente (hablando en materia de Educación) el disminuir la posibilidad de futuros ataques por falta de información y conocimiento por parte de los empleados representa un ahorro millonario a largo plazo, mayor que la inversión en educar para concientizar a los futuros líderes.

A mi parecer, un proyecto de educación visto de cualquier óptica es un beneficio. El solo hecho de incrementar los conocimientos para un fin sumamente práctico ya es una ganancia y un prestigio para los profesionales que dirigen las empresas argentinas, además que se reducirían los delitos informáticos, se incrementaría la seguridad, y podría lograrse un ahorro para el Estado.

Mejor aún, contamos con especialistas capacitados para comenzar un proyecto piloto de educación. Y creo que el resto de las provincias al ver el éxito en los resultados, van a querer extender el proyecto.

Glosario

.doc: Extensión de un archivo que identifica a un documento de texto. Es interpretada por cualquier procesador de textos.

.xls: Extensión de un archivo que identifica a una planilla de cálculos. Es interpretada por cualquier software de procesamiento de cálculos como Microsoft Excel, Open Office Calc, o GS- Calc.

Antispyware: Programa diseñado para detectar y remover software espía.

Antivirus: Programas diseñados para la detección y posible eliminación de virus informáticos.

Ataque: Acción en la que alguien rompe las reglas de seguridad y preservación de la intimidad de un sistema informático.

AWACS: Aviones utilizados por OTAN del Sistema Aerotransportado de Alerta y Control Anticipado.

Banda Ancha: Característica de una red que posee mucha capacidad y gran velocidad para la transmisión de datos.

Bases de datos: Conjunto de datos relacionados que se almacenan de forma que se pueda acceder a ellos de manera sencilla, con la posibilidad de relacionarlos, ordenarlos en base a diferentes criterios, etc.

Booteo: Término utilizado para referirse al comienzo o arranque. Si se habla del sector de booteo, entonces se refiere al sector que contiene la información necesaria para arrancar un sistema o programa.

E-mail o Casilla de correo: Dirección de correo electrónico que utiliza una persona o empresa que le permite recibir, enviar y almacenar correos.

Código fuente: Son las instrucciones contenidas en un programa a las cuales una computadora entiende por medio de un programa interprete

Dispositivos de almacenamiento: Estructuras físicas donde se guarda información, que pueden ser ópticos, magnéticos, flexibles, etc.

Exploits: Software que aprovecha alguna debilidad de un sistema operativo. Los Exploits no necesariamente son maliciosos.

Firewall o Cortafuego: Software de seguridad que impide el acceso de personas no autorizadas a una red interna desde el exterior (como puede ser Internet).

Gusano: Programa similar a un virus. No altera los archivos, simplemente reside en la memoria y tienen la capacidad de auto replicarse.

Hacker: Experto de programación, sistemas, redes en general, Internet, computadoras y no tiene intenciones malas a diferencia de lo que se escucha comúnmente. Le gusta acceder a lugares prohibidos por diversión, alimento de ego y demostrar que para él, los sistemas mas costosos son vulnerables.

Heurística de Antivirus: Técnicas empleadas por los software antivirus para el reconocimiento inteligente de códigos maliciosos (virus, gusanos, troyanos, etc).

Hoax: Mensaje de correo electrónico con contenido falso que se distribuye mediante cadenas. Su principal objetivo es obtener direcciones de correo electrónico. También busca molestar a gente y saturar la red y los servidores.

Información: Elemento fundamental que manejan los ordenadores en forma de datos binarios.

Ingeniería Social: Técnicas y métodos utilizados para engañar a las personas y conseguir información valiéndose de su ignorancia e inocencia.

Ingeniero Social: Persona con alta capacidad de convicción y facilidad para engañar a otras personas y lograr que le digan información confidencial que necesita. Este utilizara como herramientas un teléfono, una charla por chat o en el mejor de los casos lo hará personalmente.

Internet: Conjunto de redes interconectadas que permiten la comunicación entre millones de usuarios de todo el mundo. Para el acceso a ella los usuarios necesitan tener un prestador de servicios que le provea un nombre de usuario y contraseña.

Keylogger: Programa malicioso que registra cada vez que se pulsa una tecla en el teclado y se almacenan en un archivo de texto.

Link o Hipervínculo: Vínculo que sirve para ir de una sección a otra, o de una página a otra, cuando se navega por Internet o al usar planillas de cálculo o archivos de texto.

Macro: Es un grupo de comandos de un aplicación, organizados según ciertas instrucciones cuya ejecución puede ser pedida de una sola vez para la función que se desea. Lo que permite ahorrar tiempo al programador al no tener que repetir partes idénticas de un programa.

Malware o Malicious Software: Programa diseñado para hacer algún daño a un sistema. Puede presentarse en forma de virus, gusanos, caballos de Troya, etc.

Memoria USB: Dispositivo de almacenamiento portátil, de muy poco tamaño y peso. Con capacidades que van desde los 64Mb. a los 8Gb de información. La forma de transmitir la información es por medio de un conector USB que tiene en un extremo que se puede conectar a cualquier dispositivo

Password o contraseña: En español palabra clave. Código personal y privado que fue asignado previamente a un usuario determinado. Para comenzar cualquier operación esta clave es requerida.

Phishing: Técnica que consiste en utilizar algún medio de información como puede ser el correo electrónico o llamada telefónica para engañar a personas y “robarles” su dinero. Al parecer estos mensajes proceden de un negocio digno de confianza (un banco o compañía de crédito) que solicita “verificación” de los datos por un supuesto problema.

Phreaker: Personas que intentan usar la tecnología disponible para explorar y/o controlar los sistemas telefónicos sin permiso.

Portador: Archivo que sirve de transporte para los virus. Puede ser un archivo ejecutable, el sector de arranque de un disquete, etc.

Red: Conexiones que dan soporte a las comunicaciones que pueden establecer 2 o mas computadoras con el fin de compartir datos, recursos, etc.

Rootkit: Programa que utiliza un atacante luego de andar ilegalmente por un sistema, para ocultar su presencia y a su vez dejarle garantizado el ingreso en un futuro.

SMS: (Short Message Service) Servicio de mensajería para celulares.

Spam: Mensaje de correo masivo con contenido publicitario no solicitado.

Spam SMS: Spam que se difunde por dispositivos celulares mediante la tecnología SMS (mensajes de texto cortos).

Spim: Spam sobre mensajería instantánea (MSN Messenger, ICQ, etc).

Spit: Spam sobre telefonía IP.

Spyware: Software espía que se encarga de recopilar información de usuarios para luego enviarla al servidor de la empresa que le interesa conocer dicha información. Utilizado para conocer gustos de los usuarios para luego hacerles ofertas a medida.

Troyano: Programa dañino, utilizado normalmente como herramienta para espiar, que suele presentarse disfrazado o incluido dentro de otro programa. Cuando este programa es ejecutado el troyano realiza la acción prevista.

Virus: Programa maligno que infecta un sistema o unidad física de almacenamiento y tiene la capacidad de auto-replicarse. Este necesita un portador o archivo donde incluirse para poder replicarse.

Vishing: Evolución de phishing o también conocido como phishing telefónico, pero en esta caso se hace utilizando voz sobre IP (VoIP), telefonía móvil y telefonía terrestre.

VoIP: (Voice over Internet Protocol) Tecnología que permite realizar llamadas telefónicas a un muy bajo costo ya que envía la voz en forma de datos a direcciones en Internet en vez de hacerlo a un teléfono fijo).

Bibliografía

Sitios Web Consultados

Fisher, Dennis (2003) “E-Mail Hoax Targets First Union Customers”,
<http://www.eweek.com/article2/0,3959,1068224,00.asp>

The Teacher, Lester (2002) “Curso de Ingeniería Social”, <http://lestertheteacher.cjb.net>

Caruana, Pablo M. (2001) “Breves Conceptos sobre la Ingeniería Social”,
<http://virusattack.xnetwork.com.ar/articulos/VerArticulo.php3?idarticulo=4>

Fernández Gómez, Jaime (2000) “Ingeniería Social”,
<http://www.iec.csic.es/criptonomicon/articulos/expertos72.html>

McDowell, Mindi (2004) “Avoiding Social Engineering and Phishing Attacks”,
<http://www.us-cert.gov/cas/tips/ST04-014.html>

Wikipedia (2006),
<http://wikipedia.com>

Identidad Robada (2006),
<http://www.identidadrobada.com/>

Stasiukonis, Steve (2006) “The USB Way”,
http://www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1

El Mundo(2004) “El Coronel Martínez Inglés logró infiltrarse en la Boda Real”
<http://www.elmundo.es/elmundo/2004/05/24/espana/1085401631.html>

Alvy, Nacho, Wicho (2002) “Malos Usos de la Ingeniería Social”,
<http://www.microsiervos.com/archivo/seguridad/mala-ingenieria-social.html>

Harl (1997) “The Psychology of Social Engineering”, <http://lestertheteacher.cjb.net/>

Molist, Mercè (2002) “INGENIERÍA SOCIAL: Mentiras en la red”
<http://ww2.grn.es/merce/2002/is.html>
<http://ww2.grn.es/merce/2002/is.html>

Bearman, Ross (Sir Ross) (2004) “A Guide To Social Engineering – Vol.1”
<http://lestertheteacher.cjb.net>

www.cadena.ser (2004) “Operativo de Seguridad en la Boda Real”
http://www.cadenaser.com/articulo.html?xref=20040521csrsrcnac_12&type=Tes

Solomon, Alan “All About Viruses”
<http://www.drsolomon.com/vircen/allabout.html>

www.virusprot.com (2005) “TODO SOBRE SEGURIDAD EN INTERNET Y NETWORKING”
<http://www.virusprot.com/Teletipo501.html>

Villanueva, Miguel (2006) “Nuevo Estudio Sobre el Spam”
<http://www.miguelvillanueva.com/2006/09/16/nuevo-estudio-sobre-el-spam>

Borghello, Cristian (2006) “Los 10 virus mas detectados por ESET en Agosto de 2006”
<http://www.eset-la.com/company/article.php?contentID=1498>

www.segu-info.com.ar (2006) “Un Nuevo Troyano”
<http://www.segu-info.com.ar/blogger/blogger.htm>

Borghello, Cristian (2006) “Ingeniería Social (II)” http://www.segu-info.com.ar/boletin/boletin_060408.htm

Films Consultados

- Chappelle, Joe (Director); Markoff, John & Shimomura, Tsutomu (Guión), “**Takedown**” (EE.UU - 2000)
- Bielinsky, Fabián (Director y Guionista) “**Nueve Reinas**” (Argentina – Año 2000)
- Spielberg, Steven (Director); Nathanson, Jeff & Abagnale Jr., Frank (Guión), “**Catch me if you can**” (EEUU – Año 2002)

Diarios y Revistas

- Clarín, Buenos Aires, 9 de octubre de 2006, Página 36 “Denuncian Ataques de Hackers a varias Páginas Web Argentinas”
- Clarín, BsAs 11 de Octubre de 2006, Página 40, “Delitos Informáticos: Lo trataría hoy diputados”

Libros

- Mitnick, Kevin D. & Simon, William L. & Wozniak, Steve “The Art of Deception: Controlling the Human Element of Security”. John Wiley & Sons (2002). ISBN: 076454280X
- Cialdini, Robert B. , Ph. D. “Influence: The Psychology of Persuasion”. New York, Morrow(1993). ISBN: 0688128165