UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

Trabajo de fin de carrera titulado:

ESTUDIO DEL GRADO DE INCIDENCIA DE LA INGENIERÍA SOCIAL EN LA PRIMERA FASE DE LOS ATAQUES INFORMÁTICOS QUE SE REALIZAN ACTUALMENTE EN LAS EMPRESAS PRIVADAS DEL ECUADOR

Realizado por:

LUCIA GABRIELA HINOJOSA JARAMILLO

Como requisito para la obtención del título de

INGENIERIO EN SISTEMAS

QUITO, AGOSTO DE 2010

INDICE DE CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

INDICE DE ANEXOS

CAPITULO I

1. DISEÑO CONCEPTUAL DE LA INVESTIGACIÓN

En este capítulo se presentarán los aspectos más relevantes del diseño conceptual de la investigación y que constituyen elementos básicos en los que se soporta el desarrollo de la misma.

1.1. DETERMINACIÓN DEL PROBLEMA

Una de las herramientas más efectivas en la actualidad para atacar empresas y poder obtener información de las mismas es la ingeniería social, es una herramienta que todavía es desconocida en nuestro medio, no se sabe cómo funciona del todo por lo que no se han tomado medidas al respecto para prevenir este tipo de ataques y es difícil tomar contramedidas ya que el eslabón más débil en seguridad es la capacitación de los usuarios y es a quien menos atención se les presta.

El objetivo del presente proyecto es dar a conocer que es y cómo funciona la ingeniería social, los tipos de ataques, que tipo de problemas se pueden presentar y qué medidas se pueden tomar con respecto a esta herramienta tan usada hoy en día. Para esto se presentará un ejemplo práctico de cómo se llevan a cabo los ataques, así como también las políticas de seguridad que deben ser implementadas para disminuir la incidencia de los mismos en las personas que manejan la información de la empresa.

1.2. PLANTEAMIENTO DEL PROBLEMA

La ingeniería social es un problema que ha venido creciendo a través del tiempo, antes estos ataques no se realizaban con ayuda de la tecnología sino simplemente se la realizaba entre personas; pero, actualmente con el crecimiento y avance tecnológico estos ataques se presentan de manera informática, teniendo como blanco a las personas o los sistemas informáticos y valiéndose de herramientas tecnológicas.

A nadie escapa la enorme influencia que han alcanzado los sistemas de información y comunicaciones en la vida diaria de las personas y organizaciones, y la importancia que tiene su avance para el desarrollo de un país. Junto al avance de la tecnología informática y al conocimiento de la misma, así como su influencia en casi todas las áreas de la vida social, han surgido una serie de comportamientos que cada día son más comunes en todo tipo de empresas ya sean PYMES o grandes corporaciones y tienen cada vez mayores consecuencias y más complejas.

El avance de la tecnología ha facilitado las cosas no solo a las empresas sino también a los delincuentes cibernéticos o atacantes ya que hoy por hoy cuentan con herramientas que son de gran ayuda en sus ataques y su manera de obtener información; les simplifican mucho el trabajo y deben tener menores conocimientos para poder cometer delitos que pueden llegar a tener consecuencias fatales para la organización. Estos delincuentes cuentan también con varias maneras de realizar estos ataques, por lo que es realmente importante conocer sobre las mismas, como se presentan y como se podrían mitigar para no caer en ellos.

Muchas de las empresas que han sido víctimas de ataques informáticos o robo de información no denuncian o reportan estos delitos, debido a varias causas pero la más importante es que pueden perder prestigio, por lo que en nuestro país no son conocidos muchos de estos ataques y las pocas empresas que han hecho denuncias han sufrido grandes pérdidas debido a que pierden credibilidad ante sus clientes.

Una vez conocidos los grandes riesgos de ser víctima de un ataque de ingeniería social, se busca una manera de mitigar estos riesgos, para en el futuro evitar en la mayor medida posible caer dentro de estos ataques; para esto se presenta como propuesta formular una

serie de políticas de seguridad con las cuales se minimizarían la mayor cantidad de riesgos posibles.

1.3. FORMULACION DEL PROBLEMA

Cuando se piensa en ingeniería social, probablemente no se conocen los riesgos reales de ser víctima de uno de estos ataques; de la misma manera no existe la información suficiente sobre este tema ni la educación adecuada para evitar caer en estos ataques; por lo que, mientras no exista información suficiente y adecuada, la educación necesaria en cuanto a seguridades informáticas se trata dentro de todas las áreas de las empresas, las personas seguirán siendo blancos fáciles para los ingenieros sociales, el índice de ataques no disminuirá y las empresas y las personas en sí seguirán perdiendo el activo con mayor valor, la información.

1.4. PLANTEAMIENTO DE OBJETIVOS

Objetivo General:

Desarrollar una investigación que permita establecer claramente el funcionamiento de la ingeniería social y su incidencia en la seguridad de los sistemas informáticos en nuestro país.

Objetivos Específicos:

- Identificar las bases conceptuales que sustenten la incidencia de la ingeniería social como una técnica de ataque.

- Realizar un ejemplo práctico de cómo se lleva acabo un ataque de ingeniería social en nuestro medio, para determinar medidas prácticas de prevención de ataques de ingeniería social.
- Definir políticas de seguridad con respecto a la ingería social dentro del marco normativo de la seguridad informática de una organización.

1.5. JUSTIFICACION E IMPORTANCIA

Hace algunos años atrás, las actividades bancarias, la comunicación, el correo, etc., eran de carácter físico. Cuando una persona deseaba adquirir algún artículo como por ejemplo, una camisa, un libro, una máquina, etc., debía trasladarse hasta el lugar en donde se encontraba el producto que necesitaba o deseaba comprar. De igual forma al cobrar un cheque, solicitar el saldo de una cuenta o retirar dinero, se requería que la persona se trasladara hasta el banco para gestionar estas transacciones. En conclusión, se puede decir que no podía haber transacción que se realizara si la persona no se encontraba físicamente en el lugar; en este contexto, las técnicas de ataques se puede decir que eran personales, robo y falsificación de cheques, documentos, etc.

Hoy en día debido a la evolución de las tecnologías de la información y su aplicación en los procesos operativos y de negocio de las empresas, se ha viabilizado la creación de aplicaciones de negocio, portales de comercio electrónico, correo electrónico que facilitan la realización de actividades de compra y gestión bancaria. Sin embargo, también gracias a la tecnología, las personas están más expuestas a que puedan ser víctimas de ataques más sofisticados, a través de técnicas de ataques mejor elaboradas, usando lo que actualmente se ha conceptualizado como Ingeniería Social, que no es otra cosa que saber como convencer a la gente de que nos entregue información confidencial, tocando su lado sensible, con el único fin de llevar a cabo un ataque mediante el cual se realizará un fraude, robo o cualquier actividad dolosa en contra de una empresa o persona específica.

Frente a estos hechos, las empresas y las personas deben empezar a enterarse y entender los riegos y las diferentes formas en que pueden ser sorprendidas por gente inescrupulosa que cada vez más, se prepara técnicamente para cometer actos ilícitos.

Con el desarrollo de la presente tesis se pretende sintetizar las bases conceptuales en las que se basa esta forma de estafar y además hacer ciertas recomendaciones que mitiguen los riesgos a los que actualmente las empresas y las personas están expuestas, lo que será realizado por una persona que tiene los conocimientos necesarios para poder realizar políticas de seguridad que minimicen estos riesgos, quién será guiada por un profesional con la experiencia necesaria para completar el proyecto.

1.6. MARCO TEORICO

1.6.1 Antecedentes

Los antecedentes en los que se basa la presente investigación se refieren a que actualmente las personas usan computadoras y sistemas de información, los mismos que son vulnerables a las técnicas de ataque de los ingenieros sociales y que los seres humanos pueden ser persuadidos por las habilidades de los ingenieros sociales para divulgar información confidencial aún en contra de sus principios, convirtiéndose la segunda en una debilidad universal entre los seres humanos, la cual no depende de la plataforma, el sistema operativo, el hardware, el software o el tipo de equipo sobre el que funciona el sistema de información. Por consiguiente, la ingeniería social, es una poderosa herramienta en el arsenal del cyber terrorismo por lo que el personal de seguridad haría bien en tomar medidas para prevenir este tipo de ataques.

Podemos decir que la ingeniería social es el proceso por el cual una persona hace que otra cumpla con sus deseos. Este es el término usado para describir las técnicas y métodos usados por la gente que obtiene información sensible de manera indirecta, usualmente sin tener acceso legal a la información. Estas personas son conocidas como ingenieros sociales, y ellos típicamente inducen a otras personas con acceso legítimo a la información a que la divulguen.

En el ámbito de la seguridad informática, el término seguridad social es usado para describir el intento malicioso de las personas que tratan de obtener acceso a los datos e información sensible de manera ilegal. El proceso de conseguir información a través técnicas de ingeniería social implica perder habilidades técnicas que son reemplazadas con características y habilidades sociales. De cualquier manera, un ingeniero social experto puede gastar mucho tiempo obteniendo información pública que se encuentra disponible sobre su objetivo y conversando con víctimas eventuales antes de pedir acceso de manera directa a cierta información.

La ingeniería social es como realizar un ataque de otro tipo; hackear un servidor por ejemplo, la mayoría del trabajo está en la preparación, más que en el mismo esfuerzo del ataque. Por ejemplo, un ingeniero social debe ganar conocimiento sobre la organización y su estructura jerárquica estudiando documentos internos que pudieron ser encontrados buscando en la basura o usando cualquiera de las técnicas de la ingeniería social. Mediante una llamada telefónica, el ingeniero social debe determinar que el supervisor de los empleados está fuera de la ciudad y no es fácil localizarlo. Finalmente, el ingeniero social debe parecer un invitado del supervisor y pedir a un empleado en particular información sensible, sabiendo que no van a encontrar fácilmente al supervisor para confirmar la identidad del ingeniero social.

Las técnicas usadas por los ingenieros sociales varían dependiendo de varios factores, como el tiempo de respuesta, el tiempo de preparación, las circunstancias del ataque, el conocimiento entre la gente que maneja los datos y la información sensible. Los ataques de los ingenieros sociales generalmente usan una combinación de métodos, como el deseo de confiar y ayudar de las víctimas; el uso de información pública disponible, suposiciones sobre esta información o conocimiento actualizado sobre los procesos internos; y el uso de autoridad o cualquier otra artimaña para obtener la cooperación de las víctimas. Si los ingenieros sociales son hábiles usualmente tienen los conocimientos técnicos necesarios para obtener acceso a parte del sistema y necesitan el conocimiento de otras personas para poder acceder al resto del sistema.

La ingeniería social es definida también como la práctica de obtener información confidencial manipulando a los usuarios legítimos. De manera común lo que usa un ingeniero social es el teléfono o el Internet, así también las conversaciones personales forman parte del repertorio de técnicas usadas por los ingenieros sociales. Los ataques de

ingeniería social recaen en la naturaleza humana y su tendencia de confiar en los demás más que en las rígidas políticas de seguridad. En general, los profesionales de las seguridades están de acuerdo en que el eslabón más débil en la seguridad de las redes y sistemas informáticos es el ser humano; y los ingenieros sociales confirman esta teoría mediante sus exploits[1].

Una vulnerabilidad de la organización hacia la ingeniería social puede ser descrita en términos de cuán accesibles son los empleados a los contactos externos y su conocimiento sobre este tipo de ataques. Ocasionalmente, la meta de la ingeniería social es simplemente obtener una lista de nombres de los empleados, los cargos y los números telefónicos.

Después esta información será utilizada para llevar a cabo más ataques. Entonces, es más fácil para un atacante hacer ingeniería social en una organización que mostrar públicamente su estructura organizacional, de manera que está más comprometido alguien que tiene información propietaria y la misma está considerada como confidencial.

Las compañías grandes son particularmente vulnerables a los ataques de ingeniería social por que la probabilidad de interactuar con personas desconocidas aumenta. Esto hace que la posibilidad de que los empleados tengan menor posibilidad de reconocer a alguien que está tratando de llevar a cabo un ataque de ingeniería social. A veces sucede también que cuando el personal está entrenado para seguir estrictamente las órdenes de sus superiores, este personal es más vulnerable a los ataques que se realizan usando la técnica de la autoridad; esto ocurre porque es menos probable que cuestionen las órdenes de un superior.

División de la Ingeniería Social

A la ingeniería social se la divide en dos grupos: ingeniería social basada en humanos e ingeniería social basada en computadoras. En los ataques basados en humanos, los atacantes interactúan directamente con su víctima (en persona, por teléfono, vía e-mail, etc.) y la persuaden para cumplir con lo que ellos quieren. En los ataques basados en computadoras, los sistemas de computadoras son los que persuaden a la víctima a revelar información o realizar ciertas acciones. Por ejemplo, el phishing, es una técnica de ataque de la ingeniería social basada en computadoras, en el cual los ingenieros sociales envían un

[1] El significado de esta palabra se encuentra en el glosario de términos del presente documento.

e-mail a sus víctimas, fingiendo ser una entidad confiable y direccionándolas a enviar sus credenciales o haciendo que instalen algún software.

Pasos que constituyen un ataque de Ingeniería Social

Los ataques de ingeniería social tienden a seguir un proceso simple que contiene tres pasos principales: obtener información, establecer una relación y explotar esta relación.

En el paso de obtener información, el ingeniero social va a minar las fuentes de información de inteligencia pública. Esto incluye sitios Web de la organización, reportes, anuncios grupales, documentos legales públicos disponibles, anuncios de ventas y otras descripciones públicas de la gente, operaciones y sistemas de la organización. El objetivo de obtener información es elevar la habilidad del atacante para ser capaz de impresionar y convencer a cualquiera de que es parte de la organización. El éxito de este paso es directamente proporcional al monto de información pública disponible perteneciente a la organización de la víctima (por ejemplo: acrónimos, tablas organizacionales y otra información específica).

El paso de establecer una relación, consiste en que los ingenieros sociales fingen una relación con la víctima; la profundidad y la naturaleza del intento por formar una relación, depende del tipo de ataque. Este paso puede variar de una simple afirmación de ser un técnico o supervisor, a un largo y complicado disfraz donde la víctima se sienta personalmente conectada al atacante. La meta de establecer una relación es conseguir la confianza de la víctima para poder explotarla después.

En el paso de explotar la relación, se refiere a que los atacantes tratan de elevar o minimizar la parte sicológica de la víctima e intentan lograr que la víctima reaccione de una manera premeditada. En un e-mail de phishing por ejemplo, el empleado puede elevar la emoción de la víctima afirmando que la víctima ganó una gran suma de dinero. El atacante espera que esta cantidad de dinero colme a la víctima y le complazca al atacante en sus deseos. En un escenario interactivo, una vez que el atacante determina que la víctima ha alterado su estado, el agresor va a pedir a su objetivo que realice alguna acción o que revele alguna información confidencial que beneficiará al agresor. Si el estado social de la víctima ha cambiado de manera considerable (la víctima se siente extremadamente

obligada, apática, temerosa, enojada, etc.) la víctima va a cooperar con mayor facilidad con el atacante.

Los problemas de seguridad de los sistemas informáticos en las empresas no son la única causa para la ocurrencia de accesos no autorizados a la información; la manera de persuadir a las personas a través de técnicas bien elaboradas para obtener información confidencial son prácticas actuales para cometer ataques informáticos.

El ámbito de investigación del presente trabajo se basará en la evaluación del personal administrativo, técnico y usuarios finales de un par de empresas para saber cuál es el nivel de conocimiento que se tiene sobre ingeniería social para de esta manera poder minimizar el riesgo de sufrir un ataque de este tipo en función de conocer que es, como funciona y cuales son los resultados que tiene la ingeniería social mediante políticas y concienciación de usuarios tomando como base la investigación realizada en empresas de la ciudad de Quito.

La investigación se realizará en la primera fase de un ataque, es decir, la manera de obtener la información principal de las personas responsables de los servidores, sistemas, aplicaciones, etc., como nombres de usuario, contraseñas, números telefónicos, correos electrónicos, información sobre la plataforma tecnológica sobre la que está trabajando la empresa, etc., más no abarcará la parte de hackear un servidor como tal.

1.6.2 Índice de Contenidos

1.6.3 Fundamentación Teórica

La ingeniería social tiene varias definiciones, entre las que podemos encontrar:

"Es la técnica especializada o empírica del uso de acciones estudiadas o habilidosas que permiten manipular a las personas para que voluntariamente realicen actos que normalmente no harían"[2].

"Es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos".[3]

"Se denomina ingeniería social a todo artilugio, tretas y técnicas más elaboradas a través del engaño de las personas en revelar contraseñas u otra información, más que la obtención de dicha información a través de las debilidades propias de una implementación y mantenimiento de un sistema".[4]

"Son técnicas basadas en engaños que se emplean para dirigir la conducta de una persona u obtener información sensible"[5]

Podemos ver que es el método más simple y efectivo para sorprender a los usuarios de Correo Electrónico en el envío de virus, gusanos, troyanos, programas espía, capturadores de teclas digitadas (Keyloggers), etc.; adjuntan texto en el correo, de esta manera pueden obtener información asustando a los lectores de dichos correos.

Las plagas antes mencionadas emplean la ingeniería social y pesar de los esfuerzos de las autoridades competentes de la mayoría de países del mundo, para detener, atenuar o

[2] http://www.perantivirus.com/sosvirus/pregunta/ingsocial.htm

[3] http://foro.seprin.com/phpBB3/viewtopic.php?f=4&t=3293

[4] http://www.pericia.cl/news/noticias.htm

[5] http://informatech.uson.mx/glosario/i.php

exterminar son imposibles de combatir. Por lo que es muy importante la capacitación en este aspecto a los usuarios de correo electrónico; es decir se les deben enseñar cuales son las actitudes y aptitudes que deben tener para realizar mejor su trabajo en cuanto a seguridad de la información, equipos y sistemas se trata; que es lo que deben y no abrir y/o responder.

Para que la ingeniería social sea llevada acabo debe haber de por medio un ingeniero social; el mismo que es denominado como:

Cualquier persona puede convertirse en un ingeniero social, en un investigador, puede hacer que la gente haga cosas que usualmente no hace. No es difícil convertirse en un ingeniero social profesional, debe saber como persuadir e influenciar a la gente y una vez que sabe como combinar estas dos cosas tiene el perfil de un típico ingeniero social.

Alguien que usa el engaño, la influencia y la persuasión contra el personal de empresas usualmente apuntando a su información pertenece a la ingeniería social. Una manera de trabajar en las características que debe tener un ingeniero social es recogiendo ciertas partes de la información improvisando sus características, practicando crear pretextos de manera que sea más fácil conseguir cualquier información que se propusiera.

La ingeniería social toma ventaja del área más sensible de cualquier organización: el personal. La ingeniería social son “personas hackeando” y envuelve una explotación maliciosa del ser humano de naturaleza confiable para sacar información que puede ser usada para causar perjuicios.

Típicamente los ingenieros sociales se hacen pasar por alguien más para obtener información a la que ellos de otra manera no podrían tener acceso. Ellos luego toman la información obtenida de sus víctimas y causan estragos en los recursos de red, robo o eliminación de archivos, y también cometen espionaje industrial o cualquier otra forma de fraude en contra de la organización que ellos están atacando. La ingeniería social es diferente de los problemas de seguridad física.

Algunos ejemplos de ingeniería social son:

- Suplantación de personal de soporte técnico
- Suplantación de vendedores

- Suplantación de sitios Web
- Suplantación de empleados
- Llamadas telefónicas
- Envío de correos electrónicos
- Búsqueda en la basura
- Clonación de tarjetas de proximidad

Algunas veces los ingenieros sociales actúan como empleados enérgicos y que tienen muchos conocimientos, así como administradores o ejecutivos. Otras veces deben jugar el rol de empleados uniformados e ingenuos. Ellos usualmente cambian de una manera a otra, dependiendo de a quienes les estén hablando. La ingeniería social es una de las piraterías más fuertes porque esta tiene grandes habilidades para pasar como confiable para un extraño.

Muchos ingenieros sociales llevan a acabo sus ataques despacio, de esta manera no son tan obvios y no levantan sospechas. Estas personas reúnen bits de información todo el tiempo y usan esta para crear un cuadro más amplio de qué es lo que quieren conseguir con el ataque, a que están apuntando, que sistemas son los que están siendo usados por la empresa, que vulnerabilidades tienen, etc.

La mayoría de ataques de ingeniería social pueden ser llevados acabo con una breve llamada telefónica o un e-mail. Los métodos utilizados dependen del estilo y las habilidades del hacker.

Los ingenieros sociales saben que muchas organizaciones no tienen una clasificación formal de los datos sensibles y confidenciales, sistemas de control de acceso, planes de respuesta a incidentes y programas de conciencia de seguridad. Los ingenieros sociales saben mucho sobre muchas cosas tanto dentro como fuera de sus organizaciones objetivo porque ellas les ayudan en sus esfuerzos para realizar el ataque.

Las compañías más grandes que expanden sus fronteras son usualmente más atractivas para los atacantes, pero las compañías pequeñas también son atacadas. Cada uno desde las recepcionistas hasta los guardias de seguridad o el personal de TI son víctimas potenciales de la ingeniería social. Los empleados de la mesa de servicio y los call centers son

especialmente vulnerables porque están entrenados para ser útiles y comunicativos con la información. También un promedio de usuarios finales no entrenados son susceptibles de ataques. La ingeniería social tiene serias consecuencias. Como el objetivo de la ingeniería social es coaccionar a alguien para obtener su incomodidad, cualquier cosa es posible.

Efectivamente los ingenieros sociales pueden obtener la siguiente información:

- Nombres de usuarios y claves de administrador
- Insignias de seguridad o llaves de los edificios y de los centros de cómputo
- Propiedad intelectual así como también especificaciones de diseño, formulas y otra documentación de desarrollo e investigación
- Reportes financieros confidenciales
- Información privada y confidencial de los empleados
- Listas de clientes y prospectos de ventas
- Sistemas operativos que corren en las máquinas de la empresa

Si alguna información de las antes mencionada es filtrada puede causar perdidas financieras, reducir la moral de los empleados, poner el peligro la lealtad de los clientes y también crear problemas legales.

Una razón por la que es difícil protegerse de la ingeniería social es debido a que no está bien documentada porque hay tantos métodos existentes que la recuperación y protección de la información son difíciles después del ataque.

Con la ingeniería social uno nunca sabe el siguiente paso en el ataque; lo mejor que uno puede hacer es permanecer vigilante, entender la metodología de la ingeniería social y protegerse contra los ataques más comunes.

El proceso de ingeniería social es actualmente muy básico; en general los ingenieros sociales encuentran los detalles de los procesos organizacionales y sistemas de información para llevar acabo sus ataques. Con esta información ellos saben que perseguir.

Los hackers típicamente realizan ataques de ingeniería social en cuatro simples pasos:

1. Realizan búsquedas
2. Se ganan la confianza de la víctima

3. Explotan las relaciones para obtener información mediante palabras, acciones o tecnología
4. Usan la información reunida con propósitos maliciosos

Estos pasos pueden incluir sub-pasos y técnicas dependiendo de cómo se lleve acabo el ataque.

Antes de que los ingenieros sociales lleven acabo su ataque ellos deben tener una meta en mente. Este es el primer paso de un hacker en este proceso, y esta meta es algo como ya implantando en la mente del hacker. ¿Qué es lo que el hacker quiere conseguir? Qué es lo que el hacer trata de hackear? ¿Quiere la propiedad intelectual, claves de servidor o insignias de seguridad; o simplemente quiere probar que las defensas de la compañía son penetrables?

Hay solo una par de lineamientos de defensa contra la ingeniería social, aunque tengamos los sistemas de seguridad más fuertes, un usuario ingenuo o sin entrenar puede dejar al ingeniero social en la red. Nunca se debe subestimar el poder de los ingenieros sociales.

Debemos tomar muy en cuenta la siguiente frase:

"No hay parche ni antivirus para un usuario estúpido"[6]

Se deben crear políticas de seguridad que incluyan a los datos, el software, el hardware y a los empleados para proteger a la organización de estos ataques, estas políticas deben estar actualizándose continuamente y deben ser conocidas por todo el personal y los usuarios, quienes deben tener capacitación sobre las mismas y estar constantemente actualizándose en ellas.

La mejor manera de defenderse de la ingeniería social es una organización con empleados que pueden identificar y responder frente a los ataques de ingeniería social. La concienciación de los usuarios comienza con un entrenamiento inicial para cada uno y sigue con iniciativas de concienciación de seguridad para mantener las defensas de ingeniería social en la mente de cada uno.

[6] Midnick Kevin & Simon William , The art of Deception-Controlling the human Element of Security (traducción)

Los ingenieros sociales típicamente comienzan reuniendo información pública sobre sus víctimas.

Con respecto a la incidencia que tiene la ingeniería social en las empresas podemos encontrar diferentes tipos de la misma, entre las que se destacan:

Obtener información para sacar una base de datos, al obtener datos mediante ingeniería social podemos crear un base de datos y venderla a quien no debe; por ejemplo si las farmacias XXX están realizando una campaña nueva y YYY llama a la secretaria de la matriz de XXX y le dan información que no deben ellos pueden tomar estos datos, formar una base de datos y hacer una mejor publicidad de un producto similar. Para esto debemos tener restricciones al momento de dar datos de la empresa en la que trabajamos, debemos ser concientes de que tipo de información puede ser suministrada y a que personas.

Investigar que sistema operativo está corriendo en la empresa, con lo cual se podría averiguar que vulnerabilidades tiene y sería mucho más fácil poder hackear ésta, por ejemplo si encontramos que en el servidor de la empresa XX corre el sistema operativo Windows Server 2003 podemos buscar las vulnerabilidades que tiene este sistema operativo y vamos a saber por donde debemos atacar. Para esto se deben tener todos los parches del sistema operativo actualizados y en las páginas o consolas que muestran información del sistema operativo maquillar esta información de manera que se pueda engañar al ingeniero social, tener cuidado en los puertos que se tienen abiertos y en los usuarios y claves que vienen por defecto.

Desprestigiar a una empresa es otra incidencia que podemos encontrar con la ingeniería social, al momento de hacer esto la empresa perdería credibilidad, por lo tanto perdería clientes y dinero; por ejemplo si un ingeniero social averigua que la empresa YY tiene un problema financiero y lo divulga, la desprestigiaría y eso le traería serios problemas a la misma. Para evitar esto se debe mantener con mucha discreción y con seguridad la información secreta o sensible de la organización, tanto en los equipos como en las personas que la manipulan.

Otra forma de incidir en una empresa con ingeniería social es tratando de obtener nombres de usuario y claves, al momento de hacer esto se puede producir una denegación de servicios y si la organización deja de producir va a tener pérdidas económicas que van a significar mucho para ella; por ejemplo si se deniega el servicio de facturación de una

florícola se produciría una pérdida de dinero muy grande, pararían las ventas y los fletes de las flores no saldrían. Para esto se debe tener un gran control con las claves y nombres de usuario, se los debe cambiar cada cierto tiempo, deben ser contraseñas robustas y no deben estar pegadas en lugares como el teléfono, el monitor, bajo el teclado, etc. Y no deben ser divulgadas.

Mediante ingeniería social podemos obtener información sobre personal administrativo, que ocupa cargos altos en la empresa y puede realizarse algún tipo de chantaje o extorsión; por ejemplo si se encuentran fotos en la basura que comprometen al gerente de una empresa y un ingeniero social las encuentra podría pedir lo que el quisiera a cambio para no destruir su matrimonio. Po esto se debe tener cuidado con lo que se bota a la basura, que esto sea triturado, quemado y que no se tenga un fácil acceso a la basura que contiene información confidencial. Que todos los papeles, llamadas, correos, etc. que contienen este tipo de datos sean seguros, sean procesados de la manera adecuada.

Realizando uno de estos ataques se puede dar una competencia desleal, lo que puede ocasionar pérdidas para la empresa, robos de personal, de campañas publicitarias, etc.; por ejemplo si se tiene acceso a la base de datos de recursos humanos de la empresa AAA se van a ver los sueldos de los empleados e investigando cuales son los mejores se podría presentar una propuesta de trabajo para ellos con un mayor sueldo y se le quitaría a esta empresa algunos de sus mejores empleados y ocasionaría pérdidas de diferente índole para la organización. Por lo que las bases de datos deben ser seguras, no se deben copiar a menos de que sea con permisos de administrador, el mismo que debería cambiar su calve periódicamente para evitar este tipo de problemas, la base de datos no debería dejar que la copien solo arrastrándola o que la modifiquen con facilidad.

También se puede obtener información y llevar acabo una desinformación, lo que podría llegar a provocar un caos en la empresa; por ejemplo si el ejército realiza una llamada y ésta es interceptada por un ejército enemigo, con la información que obtuvo de esta llamada podría enviar un mensaje a las tropas con otra información y mandarlas a un lugar equivocado y ellos tomarían ventaja de esto. Por lo que la medida para esto sería tener mayor seguridad en las llamadas que se realizan o contestan por ejemplo tener un identificador de llamadas en cada extensión y en los mensajes que se envía tener algún mecanismo que me asegure que el mensaje no va a ser recibido por alguien que no sea su destinatario.

Por último una de las mayores incidencias que se pueden presentar con la ingeniería social es el SPAM; lo que podría provocar que las redes en la empresa colapsen o que la información del personal de la empresa sea usado con fines no apropiados; por ejemplo si llega una propaganda sobre pastillas para bajar de peso a alguna empleada de la empresa y ella abre este correo, quién envió el e-mail sabe que ella abre esta publicidad y puede tener acceso a su libreta de contactos, con lo que se podría generar la cantidad de SPAM que se quiera a las direcciones de correo que va a tener esta mujer en su libreta de contactos y esto ocuparía un gran ancho de banda de la empresa y podría darse que algunos servicios importantes no se lleven acabo porque no hay el ancho de banda suficiente. Para contrarrestar esto se debe tener un gran control en el firewall, reglas bien definidas, etc. para evitar que entre correo basura en la red de la empresa.

1.6.4 Fundamentación Legal

Dentro de la Ley de Comercio Electrónico que se encuentra vigente en el Ecuador, se pueden encontrar los siguientes artículos referentes a las informáticas.

DE LAS INFRACCIONES INFORMATICAS

Artículo 57.- Infracciones Informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente Ley.

Reformas al Código Penal

Artículo 58.- A continuación del Art. 202, inclúyanse los siguientes artículos innumerados:

"Artículo ....- El que empleando cualquier medio electrónico, informático o a fín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Artículo ...- Obtención y utilización no autorizada de Información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.".

Artículo 59.- Sustitúyase el Art. 262 por el siguiente:

"Art. 262.- Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados en razón de su cargo".

Artículo 60.- A continuación del Art. 353, agréguese el siguiente artículo innumerado:

"Art….- Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio, alteren o modifiquen mensajes de datos, o la información incluída en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;
2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;
3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.
El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo."

Artículo 61.- A continuación del Art. 415 del Código Penal, inclúyanse los siguientes artículos innumerados:

"Art.....- Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.
La pena de prisión será de tres a cinco años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculada con la defensa nacional.

Art. .....- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica.".

Artículo 62.- A continuación del Art. 549, introdúzcase el siguiente artículo innumerado:

"Art.... Apropiación ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la

apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

"Art. ….- La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

1. Inutilización de sistemas de alarma o guarda;
2. Descubrimiento o descifrado de claves secretas o encriptadas;
3. Utilización de tarjetas magnéticas o perforadas;
4. Utilización de controles o instrumentos de apertura a distancia; y,
5. Violación de seguridades electrónicas, informáticas u otras semejantes.".

Artículo 63.- Añádase como segundo inciso del artículo 563 del Código Penal el siguiente: "Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando los medios electrónicos o telemáticos".

Artículo 64.- A continuación del numeral 19 del Art. 606 añádase el siguiente:

"..... Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.".

1.6.5 Glosario de términos

- Ataque: Un ataque es un intento organizado y deliberado de una o más personas para causar daño o problemas a un sistema informático o red. Este fenómeno

mundial ha evolucionado a tal manera que resulta de una combinación de motivaciones.

- Artilugio: Mecanismo o artefacto que nos sirve para realizar una acción.

- Bits: Unidad de información más pequeña o medida de la capacidad que tiene un ordenador o computadora.

- Call center: Provee a la empresa de los elementos necesarios para, con un servicio centralizado vía telefónica, establezca relaciones de mutuo beneficio, con sus clientes, proveedores, etc.

- Centro de cómputo: Habitación en donde hay múltiples computadoras para un fin específico.

- Clave: Contraseña, combinación de signos que sirven para abrir o hacer funcionar ciertos aparatos o sistemas.

- Concientizar: Hacer que alguien sea consiente de algo, que lo conozca y sepa su alcance.

- Control de acceso: Es la habilidad de permitir o denegar el uso de un recurso particular a una entidad en particular.

- Delincuente: Persona que comete delitos.

- Delito: Crimen o violación de la ley; acción u omisión voluntaria castigada por la ley con pena grave.

- Dispositivos de autenticación: Aparatos electrónicos que nos permiten confirmar que algo es auténtico, que la identidad de una persona es verdadera.

- E-mail: Correo electrónico, es un método para crear, enviar y recibir mensajes a través de sistemas de comunicación electrónica

- Espionaje: Actividad encaminada a obtener información reservada o secreta.

- Exploits: Pieza de software, o secuencia de comandos para automatizar el aprovechamiento de un error, fallo o vulnerabilidad, a fin de causar un comportamiento no deseado o imprevisto en los programas informáticos, hardware, o componente electrónico.

- Filtrar: Hacer pasar algo por un filtro; revelar algo que debía mantenerse en secreto.

- Firewall: Herramienta de seguridad que controla el tráfico de entrada/salida de una red.

- Fraude: Engaño que se realiza eludiendo obligaciones legales o usurpando derechos con el fin de obtener un beneficio.

- Gusano: Tipo de virus que se auto replica, residiendo en memoria.

- Hackear: Acción realizada por un hacker.

- Hacker: Término utilizado para llamar a una persona con grandes conocimientos en informática y telecomunicaciones y que los utiliza con un determinado objetivo.

- Información: Conjunto de datos sobre un tema determinado.

- Jurisprudencia: Conjunto de sentencias de los tribunales y doctrinas que contienen.

- Keyloggers: Es un diagnóstico utilizado en el desarrollo de software que se encarga de registrar las pulsaciones que se realizan sobre el teclado, para memorizarlas en un fichero o enviarlas a través de Internet.

- Lineamientos: Conjunto de acciones especificas que determinan la forma, lugar y modo para llevar a cabo una política.

- Mecanismo: Modo de funcionamiento o desarrollo de algo.

- Mesa de servicio: Es un punto único para los usuarios finales que necesitan ayuda.

- Mitigar el riesgo: Disminuir en lo posible que ocurra un incidente considerado como riesgo.

- Panel de control: Ventana que permite acceder a múltiples aplicaciones y herramientas.

- Penetrable: Que es fácil de penetrar.

- Políticas: Conjunto de criterios generales que establecen el marco de referencia para el desempeño de las actividades en materia de obra y servicios relacionados con la misma.

- Política de seguridad: Es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información. Contiene la definición de la seguridad de la información bajo el punto de vista de cierta entidad. Debe ser enriquecida y compatibilizada con otras políticas dependientes de ésta, objetivos de seguridad, procedimientos, etc. Debe estar fácilmente accesible de forma que los empleados estén al tanto de su existencia y entiendan su contenido. Puede ser también un documento único o inserto en un manual de seguridad.

- Programa espía (Spyware): Es un software o programa espía que se introduce en la computadora a manera de virus para causar daño.

- Recursos de red: Son las aplicaciones, herramientas y dispositivos que pertenecen a una red.

- Riesgo: Es la probabilidad de que suceda un evento, impacto o consecuencia adversos.

- Seguridad: Técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios.

- Seguridad física: Son barreras físicas y mecanismos de control en el entorno de un sistema informático, para proteger el hardware de amenazas físicas

- Sitio Web: Es un sitio (localización) en la World Wide Web que contiene documentos (**páginas Web**) organizados jerárquicamente. Cada documento (página Web) contiene texto y o gráficos que aparecen como información digital en la pantalla de un ordenador.

- Sistemas: Conjunto de partes o elementos organizadas y relacionadas que interactúan entre sí para lograr un objetivo. Los sistemas reciben (entrada) datos, energía o materia del ambiente y proveen (salida) información, energía o materia.

- Sistema automatizado: Es la tecnología utilizada para realizar procesos o procedimientos sin la ayuda de las personas.

- Sistema de detección de intrusos: Sistema que detecta manipulaciones no deseadas en el sistema, especialmente a través de Internet. Las manipulaciones pueden ser ataques de hackers malintencionados.

- Soporte técnico: Es un grupo de servicios que proveen asistencia para hardware, software u otros bienes electrónicos o mecánicos.

- SPAM: Correo basura o no deseado que entra en una red.

- Suplantación: sustitución ilegal de una persona para obtener algún beneficio

- Tecnología informática (TI): herramientas y métodos empleados para recabar, retener, manipular o distribuir información. La tecnología de la información se encuentra generalmente asociada con las computadoras y las tecnologías afines aplicadas a la toma de decisiones

- Troyano: Es un tipo de virus que se esconde con el mismo concepto que se usó con el caballo de Troya para causar daño.

- Usuario: Que tiene derecho de usar de una cosa ajena con cierta limitación

- Víctima: Persona que padece daño por culpa ajena o por causa fortuita.

- Virus: Programa introducido subrepticiamente en la memoria de un ordenador que, al activarse, destruye total o parcialmente la información almacenada.

- Vulnerable: Que puede ser herido o recibir algún tipo de lesión.

1.7. METODOLOGIA DE LA INVESTIGACIÓN

1.7.1 Modalidad de la Investigación

La presente investigación es una investigación de campo, la misma que será apoyada por investigación bibliográfica.

1.7.2 Tipo de la Investigación

La investigación que se realizará en este proyecto es de tipo exploratoria.

1.7.3 Técnicas de Investigación

Esta investigación pretende lograr una apreciación general de las diferentes técnicas de ingeniería social que se están aplicando actualmente en nuestro entorno y debido a que la ingeniería social es una técnica no muy conocida en nuestro país, se utilizarán encuestas para conocer que tan informadas y prevenidas están las personas sobre este tema.

Una vez realizadas las encuestas se procederá con la tabulación de las mismas, el análisis de los resultados y la interpretación de los mismos.

1.8. BIBLIOGRAFIA

- Beaver Kevin “Hacking for Dummies”. Wiley Publishing, Inc. 2004
- David Gragg, “A Multi-Level Defense Against Social Engineering ” GSEC Option 1version 1.4b, December 2002
- EC-Council “Ethical Hacking” version 5, Module III, Scanning
- EC-Council “Ethical Hacking” version 5, Module IX, Social Engineering
- EC-Council “Ethical Hacking” version 5, Advanced Module, Reverse Engineering
- EC-Council “Case Studies ” Computer Hacking Forensic Investigator
- EC-Council ” ECSA/LPT” Module XXV, Social Engineering Penetration Test
- EC-Council ” ECSA/LPT” Module XXVIII, Physical Security Penetration Test
- EC-Council ” ECSA/LPT” Module XXXV, Ethics of a Licensed Penetration Test
- http://www.gestiopolis.com/canales/demarketing/articulos/61/callcenter.htm
- http://www.alegsa.com.ar/Dic/
- http://www.descargar-antivirus-gratis.com/keylogger.php
- http://www.perantivirus.com/sosvirus/pregunta/ingsocial.htm
- http://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica)
- http://www.rompecadenas.com.ar/ingsocial.htm
- http://www.tp.com.pe/teris/index.php?option=com_content&task=view&id=92&Itemid=42

- http://www.iworld.com.mx/iw_Opinions_read.asp?IWID=64
- http://www.alcancelibre.org/article.php/importancia-seguridad
- http://www.entrebits.cl/foros/zona-hackers-y-seguridad/45-ingenieria-social.html
- http://www.wordreference.com
- Mitnick Kevin & Simon William “The art of Deception”. Kineticstomp.
- http://www.sexovida.com/psicologia/pnl.htm
- http://www.gestiondeventas.com/neurolinguistica.htm
- http://www.definiciones.com.mx/definicion/M/metodologia/
- http://www.wikipedia.org
- Karen J Bannan, Internet World, Jan 1, 2001
- Richard N. Kocsis, “Criminal Profiling” Principles and Practices.
- Kevin D. Mitnick & William L. Simon, “El Arte de la Intrusión”.
- Aaron Dolan, “Social Engineering”
- David Gragg, “A Multi-Level Defense Against Social Engineering” GSEC Option 1 version 1.4b, December 2002
- Ley de Comercio Electrónico del Ecuador

CAPITULO II

2. DEFINICIONES CONCEPTUALES DE INGENIERIA SOCIAL

2.1. CONCEPTO DE INGENIERIA SOCIAL

La ingeniería social tiene varias definiciones, entre las que se puede encontrar:

- "Es la técnica especializada o empírica del uso de acciones estudiadas o habilidosas que permiten manipular a las personas para que voluntariamente realicen actos que normalmente no harían".[7]
- "Es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos".[8]
- "Se denomina ingeniería social a todo artilugio, tretas y técnicas más elaboradas a través del engaño de las personas en revelar contraseñas u otra información, más que la obtención de dicha información a través de las debilidades propias de una implementación y mantenimiento de un sistema".[9]
- "Son técnicas basadas en engaños que se emplean para dirigir la conducta de una persona u obtener información sensible".[10]

Es el proceso de engañar a la gente para obtener información confidencial, privada o privilegiada o de acceso para un hacker.[11] Realmente no hay mucha diferencia entre las

[7] http://www.perantivirus.com/sosvirus/pregunta/ingsocial.htm

[8] http://foro.seprin.com/phpBB3/viewtopic.php?f=4&t=3293

[9] http://www.pericia.cl/news/noticias.htm

[10] http://informatech.uson.mx/glosario/i.php

[11] Midnick Kevin & Simon William , The art of Deception-Controlling the human Element of Security (traducción)

técnicas usadas para la ingeniería social y las técnicas usadas para llevar a cabo un fraude tradicional**.**

Un ingeniero social es un hacker que usa el cerebro en lugar de la fuerza de la computadora. Los hackers llaman a los centros de datos y pretenden ser clientes que han perdido sus claves o se presenta en un lugar simplemente esperando a alguien que tenga una puerta abierta para ellos. Otras formas de ingeniería social no son tan obvias. Los hackers han sido conocidos por crear sitios web, concursos o cuestionarios que le piden a un usuario que ingrese su clave.

La ingeniería social es irrumpir en una red corporativa desde el lado humano.

Las compañías con procesos de autenticación, firewalls, redes privadas virtuales y software de monitoreo de red todavía están expuestas a ataques.

Un empleado sin intención puede dar información clave mediante correos electrónicos o respuestas telefónicas a alguien que no conoce o conversando con compañeros de trabajo en un bar después de las horas laborables.

Las tácticas o trucos de obtener información sensible explotando cosas básicas de la naturaleza humana como:

- Miedo
- Confianza
- Deseo de ayudar

La ingeniería social trata de obtener información como:

- Información sensible
- Detalles de autorización
- Detalles de acceso

Usualmente el eslabón más débil de cadena son las personas.

Una defensa exitosa depende de tener unas buenas políticas y de educar a las personas en como seguirlas.

La ingeniería social es el ataque más difícil del que hay que defenderse porque no puede ser defendido solo con software o hardware.

Los hackers usan términos como “Rebeca” y “Jésica” para denotar sus ataques de ingeniería social.

Ellos usan estos términos habitualmente con las víctimas de estos ataques.

Rebeca y Jésica hablan sobre una persona que es un blanco fácil sobre el cual llevar a cabo un ataque de ingeniería social, como la recepcionista de una compañía.

Por ejemplo:

- Había una Rebeca en el barco y yo le voy a llamar para obtener información privilegiada.
- Conocía a una señorita Jésica que era un blanco fácil para aplicarle ingeniería social.
- Hay alguna Jésica trabajando en su compañía?

A pesar de tener el mejor firewall, sistemas de detección de intrusos y antivirus que la tecnología tiene para ofrecer todavía existen incumplimientos de seguridad.

Una razón para esto puede ser la carencia de conocimiento entre los empleados.

Los hackers pueden intentar obtener información sensible mediante ingería social realizada a los empleados de una oficina, por ejemplo:

- Políticas de seguridad
- Documentos sensibles
- Infraestructura de red de la oficina
- Claves

Algunos ejemplos de ingeniería social son:

- Suplantación de personal de soporte técnico
- Suplantación de vendedores
- Suplantación de sitios Web

- Suplantación de empleados
- Llamadas telefónicas
- Envío de correos electrónicos
- Búsqueda en la basura
- Clonación de tarjetas de proximidad

Con la ingeniería social uno nunca sabe el siguiente paso en el ataque; lo mejor que se puede hacer es permanecer vigilante, entender la metodología de la ingeniería social y protegerse contra los ataques más comunes.

El proceso de ingeniería social es actualmente muy básico; en general los ingenieros sociales encuentran los detalles de los procesos organizacionales y sistemas de información para llevar a cabo sus ataques. Con esta información ellos saben que perseguir.

Hay solo una par de lineamientos de defensa contra la ingeniería social, aunque tengamos los sistemas de seguridad más fuertes, un usuario ingenuo o sin entrenar puede dejar al ingeniero social en la red. Nunca se debe subestimar el poder de los ingenieros sociales.

Debemos tomar muy en cuenta la siguiente frase:

"No hay parche ni antivirus para un usuario estúpido"[12]

Se deben crear políticas de seguridad que incluyan a los datos, el software, el hardware y a los empleados para proteger a la organización de estos ataques, estas políticas deben estar actualizándose continuamente y deben ser conocidas por todo el personal y los usuarios, quienes deben tener capacitación sobre las mismas y estar constantemente actualizándose en ellas.

La mejor manera de defenderse de la ingeniería social es una organización con empleados que pueden identificar y responder frente a los ataques de ingeniería social. La concienciación de los usuarios comienza con un entrenamiento inicial para cada uno y sigue con iniciativas de concienciación de seguridad para mantener las defensas de ingeniería social en la mente de cada uno.

[12] International Council of e-commerce consultants, Ethical Hacking Version 5, Module IX, Social Engineering (Traducción)

Los ingenieros sociales típicamente comienzan reuniendo información pública sobre sus víctimas.

Con respecto a la incidencia que tiene la ingeniería social en las empresas se puede encontrar diferentes tipos de la misma, entre las que se destacan:

Obtener información para sacar una base de datos, al obtener datos mediante ingeniería social se puede crear un base de datos y venderla a quien no debería tener acceso a esta información; por ejemplo si las farmacias X están realizando una campaña nueva y la farmacia Y llama a la secretaria de la matriz de X y esta persona proporciona información confidencial a las personas de la farmacia Y, las mismas pueden tomar los datos obtenidos, utilizarlos para formar una base de datos y hacer una mejor publicidad de un producto similar. Para esto se debe tener restricciones al momento de dar datos de la empresa en la que trabajamos, debemos ser consientes de que tipo de información puede ser suministrada y a qué personas.

Investigar el sistema operativo que está corriendo en la empresa, con lo cual se podría averiguar qué vulnerabilidades tiene y sería mucho más fácil poder explotarlas. Por ejemplo si se encuentra que en el servidor de la empresa X corre el sistema operativo Windows Server 2003 podemos buscar las vulnerabilidades que tiene este sistema operativo y se puede saber por donde debemos atacar. Para esto se deben tener todos los parches del sistema operativo actualizados y en las páginas o consolas que muestran información del sistema operativo maquillar esta información de manera que se pueda engañar al ingeniero social, tener cuidado en los puertos que se tienen abiertos y en los usuarios y claves que vienen por defecto.

Desprestigiar a una empresa es otra incidencia que se puede encontrar con la ingeniería social, al momento de hacer esto la empresa perdería credibilidad, por lo tanto perdería clientes y dinero; por ejemplo si un ingeniero social averigua que la empresa Y tiene un problema financiero y lo divulga, la desprestigiaría y eso le traería serios problemas a la misma. Para evitar esto se debe mantener con mucha discreción y con seguridad la información secreta o sensible de la organización, tanto en los equipos como en las personas que la manipulan.

Otra forma de incidir en una empresa con ingeniería social es tratando de obtener nombres de usuario y claves, al momento de hacer esto se puede producir una denegación de

servicios y si la organización deja de producir va a tener pérdidas económicas importantes; por ejemplo si se deniega el servicio de facturación de una florícola se produciría una pérdida de dinero, pararían las ventas y los fletes de las flores no saldrían. Para esto se debe tener un gran control con las claves y nombres de usuario, se los debe cambiar cada cierto tiempo, deben ser contraseñas robustas y no deben estar pegadas en lugares como el teléfono, el monitor, bajo el teclado, etc., y no deben ser divulgadas.

Mediante ingeniería social se puede obtener información sobre personal administrativo, que ocupa cargos altos en la empresa y puede realizarse algún tipo de chantaje o extorsión; por ejemplo si un ingeniero social encuentra un correo electrónico impreso en la basura que contenga datos personales o información confidencial del gerente de una empresa podría pedir utilizar todos estos datos o información para llevar a cabo un ataque informático. Por esto se debe tener cuidado con lo que se bota a la basura, que esto sea triturado, quemado y que no se tenga un fácil acceso a la basura que contiene información confidencial. Que todos los papeles, llamadas, correos, etc. que contienen este tipo de datos sean seguros y sean procesados de la manera adecuada.

Realizando uno de estos ataques se puede dar una competencia desleal, lo que puede ocasionar pérdidas para la empresa, robos de personal, de campañas publicitarias, etc.; por ejemplo si se tiene acceso a la base de datos de recursos humanos de la empresa A, se pueden conocer los sueldos de los empleados e investigando cuales son los mejores, se podría presentar una propuesta de trabajo para ellos con un mayor sueldo y se le quitaría a esta empresa algunos de sus mejores empleados y ocasionaría pérdidas de diferente índole para la organización. Por lo que las bases de datos deben ser seguras, no se deben copiar a menos de que sea con permisos de administrador, el mismo que debería cambiar su clave periódicamente para evitar este tipo de problemas o que la modifiquen con facilidad, debe existir pistas de auditoria.

También se puede obtener información y llevar acabo una desinformación, lo que podría llegar a provocar un caos en la empresa; por ejemplo si el ejército realiza una llamada y ésta es interceptada por un ejército enemigo, con la información que obtuvo de esta llamada podría enviar un mensaje a las tropas con otra información y mandarlas a un lugar equivocado y ellos tomarían ventaja de esto. Por lo que, la medida para esto sería tener mayor seguridad en las llamadas que se realizan o contestan por ejemplo tener un identificador de llamadas en cada extensión y en los mensajes que se envía tener algún

mecanismo que me asegure que el mensaje no va a ser recibido por alguien que no sea su destinatario.

Por último una de las mayores incidencias que se pueden presentar con la ingeniería social es el SPAM, lo que podría provocar que las redes en la empresa colapsen o que la información del personal de la empresa sea usado con fines no apropiados. Por ejemplo si llega una propaganda sobre pastillas para bajar de peso a alguna empleada de la empresa y ella abre este correo, quién envió el e-mail sabe que ella abre esta publicidad y puede tener acceso a su libreta de contactos, con lo que se podría generar una gran cantidad de SPAM dirigida a las direcciones de correo que va a tener esta mujer en su libreta de contactos y esto ocuparía un gran ancho de banda de la empresa, ocasionando que algunos servicios importantes no se lleven a cabo porque no se dispone del ancho de banda suficiente. Para contrarrestar esto se debe tener un gran control en los dispositivos periféricos, reglas bien definidas, etc. para evitar que entre correo basura en la red de la empresa.

2.2. CONCEPTO DE NEUROLINGÜÍSTICA

La Neurolingüística estudia los mecanismos del cerebro humano que posibilitan la comprensión, producción y conocimiento del lenguaje, ya sea hablado, escrito o con signos.[13]

Es una ciencia actual que integra las características psicológicas y genera un puente para ponerlas a disposición de la negociación personal, esta técnica fue integrada con los modelos de gente exitosa y el desagregado de sus virtudes, para modelarlas en el resto de las personas, generando un vínculo entre las cuestiones psicológicas y hechos reales,

[13] http://es.wikipedia.org/wiki/Neuroling%C3%BC%C3%ADstica

permitiendo un mayor conocimiento propio de la persona y mayor nivel de detalle de las actitudes, gestos y posturas de los potenciales clientes.[14]

Esta ciencia busca integrar a la persona en un todo, poniéndola al servicio de sus deseos y permite influir sobre el otro de una manera muy sutil, manteniendo los mismos preceptos de la venta con una actitud más perceptiva de la situación desde donde se encuentra una negociación y hacia donde se pretende llevarla en la posición futura.

La neurolingüística puede presentarse mediante varios canales de comunicación, los cuales son los siguientes:

- Visuales: Es aquel en que predomina el "ver", tendencia a dibujar en el espacio los objetos que describe, con palabras de referencia visual. Suele hablar rápido y mirar directamente a los ojos.
- Auditivo: La persona con este canal más desarrollado, suele ser conversador y es muy sensible a las entonaciones de la voz. Cuando habla no siempre mira al interlocutor y manifiestan predilección por el canal auditivo.
- Quinestésico: Las personas que priorizan este canal, dan una gran importancia a sus sensaciones, en general sus posturas son distendidas y habla lentamente con predominancia de registros graves. Es importante manejar su aspecto afectivo y las emociones.

Debido a su naturaleza interdisciplinaria, la lingüística, la neurobiología, y la lingüística computacional, entre otras, participan aportando diversas técnicas experimentales, así como perspectivas teóricas marcadamente distintas.

Históricamente, el término neurolingüística se ha asociado a menudo con el estudio de las afasias, el estudio de las carencias lingüísticas causadas por formas específicas de daño cerebral.

Aunque la afasiología es la base histórica de la neurolingüística, durante los últimos años este campo se ha desarrollado considerablemente y nuevas tecnologías se han ido incorporando a la disciplina. El lenguaje es un tema de interés central para la neurología

[14] http://www.gestiondeventas.com/neurolinguistica.htm

cognitiva, y las modernas técnicas de imagen cerebral han contribuido considerablemente a un mayor entendimiento de la organización anatómica de las funciones del lenguaje.

2.3. MOTIVACIÓN DE LA INGENIERÍA SOCIAL

Hay una variedad de cosas que motivan a la gente a llevar acabo un ataque de ingeniería social, las que incluyen pero no se limitan a:

- Ganancias financieras: Por varias razones un individuo debe llegar a obtener ganancias monetarias. Por ejemplo, él debe creer que merece más dinero del que gana o tal vez haya una necesidad de satisfacer un hábito de apostador compulsivo.
- Intereses personales: Un individuo puede, por ejemplo querer accesar y/o modificar información que está asociada con un miembro de la familia, amigo o vecino.
- Venganza: Por razones solo conocidas por el individuo, él puede ver como objetivo a un amigo, colega, organización o a un completo extraño para satisfacer el deseo emocional de vengarse de alguien.
- Presiones externas. Un individuo puede estar recibiendo presión de amigos, familiares o sindicatos de crimen organizado por razones como ganancias financieras, intereses personales o venganza.

2.4. PORQUÉ ES TAN EFECTIVA LA INGENIERÍA SOCIAL?

La efectividad de la ingeniería social se debe a ciertos factores que son los siguientes:

- Las políticas de seguridad son tan fuertes como su vínculo más débil y como se había mencionado antes, los humanos son el eslabón más débil.
- Es difícil detectar cuando se trata de hacer un ataque de ingeniería social.
- No hay un método que asegure que se tiene una seguridad completa contra los ataques de ingeniería social.
- No hay software o hardware específico contra estos ataques.

2.5. CONCEPTO DE INGENIERO SOCIAL

Cualquier persona puede convertirse en un ingeniero social, en un investigador, puede hacer que la gente haga cosas que usualmente no hace. No es difícil convertirse en un ingeniero social profesional, debe saber como persuadir e influenciar a la gente y una vez que sabe como combinar estas dos cosas tiene el perfil de un típico ingeniero social.

Alguien que usa el engaño, la influencia y la persuasión contra el personal de empresas usualmente apuntando a su información pertenece a la ingeniería social. Una manera de trabajar en las características que debe tener un ingeniero social es recogiendo ciertas partes de la información improvisando sus características, practicando crear pretextos de manera que sea más fácil conseguir cualquier información que se propusiera.

La ingeniería social toma ventaja del área más sensible de cualquier organización: el personal. La ingeniería social son “personas hackeando” y envuelve una explotación maliciosa del ser humano de naturaleza confiable para sacar información que puede ser usada para causar perjuicios.

Típicamente los ingenieros sociales se hacen pasar por alguien más para obtener información a la que ellos de otra manera no podrían tener acceso. Ellos luego toman la información obtenida de sus víctimas y causan estragos en los recursos de red, robo o eliminación de archivos, y también cometen espionaje industrial o cualquier otra forma de

fraude en contra de la organización que ellos están atacando. La ingeniería social es diferente de los problemas de seguridad física.

Algunas veces los ingenieros sociales actúan como empleados enérgicos y que tienen muchos conocimientos, así como administradores o ejecutivos. Otras veces deben jugar el rol de empleados uniformados e ingenuos. Ellos usualmente cambian de una manera a otra, dependiendo a quienes se dirijan. La ingeniería social es una de las piraterías más fuertes porque esta tiene grandes habilidades para pasar como confiable para un extraño.

Muchos ingenieros sociales llevan a cabo sus ataques despacio, de esta manera no son tan obvios y no levantan sospechas. Estas personas reúnen bits de información todo el tiempo y usan esta para crear un cuadro más amplio de qué es lo que quieren conseguir con el ataque, a qué están apuntando, qué sistemas son los que están siendo usados por la empresa, qué vulnerabilidades tienen, etc.

Los ingenieros sociales saben que muchas organizaciones no tienen una clasificación formal de los datos sensibles y confidenciales, sistemas de control de acceso, planes de respuesta a incidentes y programas de conciencia de seguridad. Los ingenieros sociales saben mucho sobre muchas cosas tanto dentro como fuera de sus organizaciones objetivo porque ellas les ayudan en sus esfuerzos para realizar el ataque.

Las compañías más grandes que expanden sus fronteras son usualmente más atractivas para los atacantes, pero las compañías pequeñas también son atacadas. Cada uno desde las recepcionistas hasta los guardias de seguridad o el personal de TI son víctimas potenciales de la ingeniería social. Los empleados de la mesa de servicio y los call centers son especialmente vulnerables porque están entrenados para ser útiles y comunicativos con la información. También un promedio de usuarios finales no entrenados son susceptibles de ataques. La ingeniería social tiene serias consecuencias. Como el objetivo de la ingeniería social es coaccionar a alguien para obtener su incomodidad, cualquier cosa es posible.

Efectivamente los ingenieros sociales pueden obtener la siguiente información:

- Nombres de usuarios y claves de administrador
- Insignias de seguridad o llaves de los edificios y de los centros de cómputo

- Propiedad intelectual así como también especificaciones de diseño, fórmulas y otra documentación de desarrollo e investigación
- Reportes financieros confidenciales
- Información privada y confidencial de los empleados
- Listas de clientes y prospectos de ventas
- Sistemas operativos que corren en las máquinas de la empresa

Si alguna información de las antes mencionada es filtrada, puede causar pérdidas financieras, reducir la moral de los empleados, poner en peligro la lealtad de los clientes y también crear problemas legales.

Los hackers típicamente realizan ataques de ingeniería social en cuatro simples pasos:

5. Realizan búsquedas
6. Se ganan la confianza de la víctima
7. Explotan las relaciones para obtener información mediante palabras, acciones o tecnología
8. Usan la información reunida con propósitos maliciosos

Estos pasos pueden incluir sub-pasos y técnicas dependiendo de cómo se lleve a cabo el ataque.

Antes de que los ingenieros sociales lleven a cabo su ataque, ellos deben tener una meta en mente. Este es el primer paso de un hacker en este proceso, y esta meta es algo como ya implantando en su mente. ¿Qué es lo que el hacker quiere conseguir? Qué es lo que el hacker trata de hackear? ¿Quiere la propiedad intelectual, claves de servidor o insignias de seguridad; o simplemente quiere probar que las defensas de la compañía son penetrables?

2.6. RASGOS COMUNES EN LOS INGENIEROS SOCIALES

Hay ciertos rasgos que son comunes en los ingenieros sociales o agresores y en las víctimas u objetivos, entre los que se puede encontrar:

- El desplazamiento de responsabilidades lejos del objetivo, de manera que el objetivo no sea considerado como único responsable por sus acciones.
- El objetivo percibe que conforme al requerimiento va a estar en el "lado correcto" de alguien que puede premiarlo por sus futuros beneficios, esto es comúnmente conocido como "ganarse al jefe".
- El instinto del objetivo para actuar moralmente, ayudando a alguien, así evitará el sentimiento de culpa.
- Comunicación en un nivel personal, la misma que resulta en el cumplimiento voluntario del requerimiento por parte del objetivo sin notar la presión que ha sido ejercida.
- El objetivo cree que está tomando una decisión razonable a cambio de una pequeña pérdida de tiempo y energía.
- La probabilidad de la complacencia del objetivo aumenta si:
    - El agresor es capaz de evadir conflictos usando un acercamiento consultivo en lugar de uno conflictivo.
    - El agresor es capaz de desarrollar y construir una relación mediante tratos previos. El objetivo probablemente cumplirá con él mediante un amplio requerimiento cumpliendo previamente con uno más pequeño.
    - El agresor es capaz de apelar a los sentidos del objetivo, como una visión o sonido. Apelando a algunos sentidos, el agresor va a ser capaz de construir una mejor relación con el objetivo mostrándose "humano" en lugar de solo un mensaje de voz o un e-mail.
    - El agresor tiene una mente rápida y es capaz de comprometerse.

2.7. SEÑALES DE AVISO CUANDO SE LLEVA A CABO UN ATAQUE

Hay varias señales que pueden ser un aviso cuando se está llevando a cabo un ataque de ingeniería social, entre estas se puede encontrar las siguientes:

- Un atacante debe mostrar incapacidad para dar el número del re-llamado válido.
- Un atacante debe hacer preguntas informales.
- Un atacante debe reclamar autoridad.
- Un atacante debe mostrar apuro o prisa.
- Un atacante debe alabar o premiar usualmente.
- Un atacante debe mostrarse incómodo cuando es cuestionado.
- Un atacante debe dar su nombre inadvertidamente.
- Un atacante debe amenazar de manera muy fuerte si la información solicitada no es entregada.

CAPITULO III

3. TIPOS Y TÉCNICAS DE INGENIERÍA SOCIAL

La ingeniería social ha desarrollado varias formas para persuadir e influenciar en las personas, para simular actos, eventos o procesos con el fin de obtener información confidencial de empresas o personas específicas; por ello es importante conocer y analizar los tipos de ingeniería social que hasta el momento se han documentado y que pueden servir de referencia para estructurar políticas de seguridad adecuadas que minimicen los riesgos informáticos.

En base a los diversos tipos de ingeniería social se han desarrollado varias técnicas para llevar a cabo un sin número de ataques; por lo que es importante conocer estás técnicas y sobre todo analizarlas, a fin de que las políticas de seguridad que se implementen o se recomienden, tengan el sustento conceptual de estas técnicas de ataque.

3.1. INGENIERÍA SOCIAL BASADA EN HUMANOS

La ingeniería social basada en humanos busca obtener información sensible mediante interacciones, es decir el ingeniero social entabla una relación con el objetivo o alguien cercano al mismo y de esta manera obtiene la información que desea.

Los ataques de esta naturaleza explotan la confianza, el miedo y el deseo de ayudar, que por naturaleza, tenemos los humanos.

Los ingenieros sociales saben exactamente como explotar esta parte humana, saben cómo llegar a las personas y hacer que ellos actúen de la manera que más les conviene. Por ejemplo el atacante adopta la identidad de una persona con autoridad, él simula una llamada a la mesa de servicios y pretende ser un Gerente y dice que ha olvidado su clave y necesita que la restauren enseguida. La persona de la mesa de servicios la restaura y le da la nueva contraseña a la persona que espera en la línea. En un tiempo mínimo el individuo puede tener acceso al sistema de personal como si él fuera el administrador y obtener los números del seguro social de quien él desee y otra información confidencial o privada de muchos empleados. Él por supuesto, podría causar más daños a la red desde que tiene acceso directo hacia ella.

Dentro de las técnicas de ataque que se puede encontrar en la ingeniería social están las técnicas por comportamiento humano, dentro de las cuales tenemos las que se detallan a continuación.

3.1.1 Ingeniería Social Inversa (Reverse Social Engineering)

Una de las técnicas usadas con mucha frecuencia por los atacantes es la conocida como ingeniería social inversa. Esto sucede cuando el hacker causa problemas en la red de la empresa objetivo o en una computadora y luego hace que él/ella mismo vaya a solucionar el problema. Una vez que el atacante ha solucionado el “problema”, él o ella son percibidos como un héroe y ha ganado así la confianza y seguridad del objetivo.

Para que la ingeniería social inversa funcione, el hacker debe ser capaz de entrar en una computadora o sistema adelantado o enviar un archivo para originar el problema. Esto requiere una buena preparación e investigación para poder alcanzar el objetivo teniendo éxito.

Por ejemplo: Ingresa el hacker a la empresa A, estudia la red que tienen, su topología, sus conexiones y enlaces, escanea los puertos abiertos y todo lo relacionado con dicha red, estudia a los empleados que la usan, quienes conocen como manejarla y quienes desconocen; de modo que cuando encuentra a alguien que es ingenuo o que no tiene conocimientos sobre el manejo o uso de la red lo vuelve su blanco. Llega un día y sin que nadie lo vea causa algún daño en la sección de la red de dicha persona, se queda sin sistema y tiene mil cosas que hacer, de manera casual llega el atacante y en su desesperación muy gentilmente le ayuda y le soluciona su problema, él o ella totalmente agradecido queda en deuda con el hacker, quien puede hacer uso de esto cuando y como desee.

- La ingeniería social inversa implica:
  - *Sabotaje*.- Después de ganar accesos simples, el atacante también corrompe la estación de trabajo o le da una apariencia de estar corrompida. El usuario del sistema descubre el problema y trata de conseguir ayuda.
  - *Marketing*.- Para asegurarse el atacante llama al usuario y el atacante proveerá información. El atacante puede hacer esto dejando su tarjeta de negocios cerca de la oficina del objetivo y/o poniendo su número de contacto en el propio mensaje.

Proveer soporte.- Finalmente, el atacante debe asistir con el problema, asegurando que el usuario no recuerde ni sospeche mientras el atacante obtiene la información requerida.

Algunos de los pros y los contras que podemos encontrar en la ingeniería social inversa y la ingeniería social son:

- IS: El hacker realiza las llamadas y depende del usuario.
- ISI: El usuario realiza las llamadas y depende del hacker.

- IS: El usuario siente que el hacker está en deuda con él.
- ISI: El usuario se siente en deuda con el hacker.

- IS: Siempre quedan preguntas sin resolver para la víctima.
- ISI: Todos los problemas son corregidos, sin levantar sospechas.

- IS: El usuario tiene control proveyendo la información.
- ISI: El hacker tiene completamente el control.

- IS: No se requiere preparación.
- ISI: Se necesita mucha planeación y acceso previos usualmente.

3.1.2 Desarrollar Confianza (Establishing Trust)

El objetivo principal en esta metodología de ataque como su nombre lo indica es establecer confianza con el objetivo; una vez que la confianza ha sido establecida el atacante podrá empezar a adquirir información sensible y el acceso necesario para irrumpir en el sistema de la empresa objetivo. El atacante, quien ya tiene una amplia experiencia va a obtener información de manera lenta pidiendo simplemente favores pequeños o pidiendo información a través de conversaciones aparentemente inocentes.

El atacante va a trabajar duro para mantener una relación que aparenta ser inocente, mientras aprende el movimiento de la organización, nombres del personal clave, los nombres de los servidores importantes, sus aplicaciones y el host de otra información valiosa.

La ingeniería social es exitosa generalmente porque los seres humanos por naturaleza brindan su ayuda a quien se la pide o solicitan ayuda cuando ellos la necesitan.

La mayoría de personas, especialmente en departamentos como Servicio al Cliente, Mesa de Ayuda o en posiciones de servicio como asistente de negocios y secretarias están

siempre listas para ayudar. Estos trabajos requieren ayudar a la gente todo el día y no es natural cuestionar la validez de cada llamada.

"Confianza, tan difícil de ganar y tan fácil de perder"[15], la confianza es la esencia de la ingeniería social.

La mayoría de humanos confía en los otros humanos hasta que se presenta una situación que influencia para que esto sea así. Se busca la ayuda de unos a otros, especialmente si la confianza puede ser construida y el requerimiento de ayuda es razonable. Mucha gente quiere ser compañero en el lugar de trabajo y no sabe que puede pasar si divulga demasiada información a una fuente "confiable". Esto se debe a que la ingeniería social puede estar inmersa en esto. Por supuesto, crear confianza toma su tiempo; los ingenieros sociales son tan astutos que logran esto en cuestión de minutos u horas. La pregunta es, ¿cómo ellos logran construir este tipo de confianza? Y esta pregunta puede encontrar la respuesta en lo siguiente:

Amabilidad: ¿Quién no se relaciona con una persona simpática? Todos amamos la cortesía. Los ingenieros sociales son muy amigables lo que les da la oportunidad de conseguir lo que se proponen. Los ingenieros sociales por lo general empiezan estableciendo intereses en común; ellos usan información que han obtenido en la fase de investigación para determinar que le gusta a la víctima y actuar si a ellos les gustan las mismas cosas. Para comenzar, ellos pueden llamar a las víctimas o reunirse con ellos en persona basándose en la información que ellos han obtenido sobre el objetivo, empiezan a hablar sobre deportes o equipos locales o cuan maravilloso es ser soltero otra vez. Unos cuantos pequeños pero bien definidos y articulados comentarios pueden ser el comienzo de una buena y linda relación.

Credibilidad: La credibilidad en cierta manera se basa en el conocimiento que tienen los ingenieros sociales y qué tan amables sean ellos. A pesar de esto, los ingenieros sociales también usan la personificación, tal vez asumiendo el papel de un nuevo

- [15] Mitnick Kevin & Simon William "The art of Deception". Kineticstomp.

empleado o un compañero de trabajo que la víctima no conoce; ellos pueden personificar a un vendedor que hace negocios con la compañía, ellos modestamente dicen tener autoridad para influenciar a la gente. El truco más común en un ingeniero social es hacer algo lindo entonces la víctima se siente obligada a ser recíproca o a ser un buen compañero en el trabajo.

3.1.3 Afectividad (Strong Affect)

La afectividad es un gatillo que usa un estado emocional elevado que habilita a un hacker para huir con más de lo que sería razonable. Si el objetivo o blanco se siente fuertemente sorprendido, impresionado o enfadado, la víctima probablemente va a pensar en los argumentos que han sido presentados para que él llegue a ese estado.

La afectividad incluye, pero no está limitada a: miedo, emoción o pánico. Esta puede ser la promesa de un premio sustancial con un valor de cientos de miles de dólares o el pánico de tener un empleado en el trabajo dependiente de una decisión. La ola de emociones fuertes trabaja como una poderosa distracción e interfiere con la habilidad de la víctima para evaluar, pensar de manera lógica o desarrollar argumentos.

El pensamiento contrafáctico es un fenómeno relacionado a la afectividad. Pensar de manera contrafáctica aumenta las posibilidades como ésta, ganar un gran premio de pequeños circuitos del pensamiento razonable de una persona. La persona ignora el hecho de que la posibilidad de ganar es de hecho muy remota, llevando a la persona a un riesgo real y bienes valiosos (información o accesos) por la posibilidad de ganar el premio. Esto es como si la persona está bajo un hechizo que ha sido sacado por la prisa de las emociones.

Los sitios web de los hackers enfatizan en el uso de la sorpresa. Las sorpresas pueden ser llevadas a cabo llamando temprano en la mañana, llegando con circunstancias o

argumentos inusuales. Las sorpresas también pueden ser obtenidas usando palabras o imágenes cargadas emocionalmente.

3.1.4 Sobrecarga (Overloading)

Las premisas erróneas suelen ser contestadas cuando se escuchan rápidamente y son intercaladas entre trivialidades convincentes. Este es un gatillo psicológico de sobrecarga. Tener que tratar con mucha información de forma rápida afecta la funcionalidad lógica y puede producir sobrecarga sensorial. Con demasiada información procesada la gente llega a ser mentalmente pasiva, es decir, ellos absorben información en lugar de evaluarla.

Defenderse de una perspectiva inesperada también puede gatillar sobrecarga. El objetivo necesita tiempo para procesar la nueva perspectiva para poder responder adecuadamente, pero este tiempo no está disponible.

Esto deja al objetivo con mucha información y con poco tiempo para pensar en la misma, mediante la reducción de la habilidad del objetivo para procesar o escrutar el argumento. El blanco luego está más dispuesto a aceptar los argumentos que han debido ser desafiados.

3.1.5 Reciprocidad (Reciprocation)

Hay una regla bien conocida en las interacciones sociales, si alguien nos da algo o nos ofrece algo nosotros debemos devolverle el favor. Esto tiende a ser verdad aun cuando el

regalo original no fue pedido o aun cuando lo que se pide a cambio es más valioso que lo que se dio originalmente. Esta verdad es conocida como “reciprocidad”.

Se ha podido observar que hay un gran uso de este gatillo psicológico. Kevin Mitnick, un hacker muy conocido, describe las reacciones que él ha visto, “En el ambiente corporativo, la gente improbablemente evalúa un requerimiento completamente, ellos solo toman un atajo mental…” El razonamiento se presenta de la siguiente manera; si alguien llama y me está ayudando con un problema, esta persona está de mi lado y esto significa que no hay peligro para mí.

La ingeniería social inversa hace uso del gatillo de reciprocidad. El hacker aparece como un héroe listo, deseoso y dispuesto a solucionar el problema del objetivo. Aun antes de que el problema haya sido resuelto el blanco se siente en deuda con el atacante. Esta es, por supuesto la situación ideal para el hacker.

Otra forma en la que la reciprocidad puede ser utilizada ha sido demostrada por experimentos de comportamiento. Estos experimentos muestran que cuando dos personas están en desacuerdo, si una se va a rendir en algún punto (no importan cuan pequeño sea) el otro se va a ver forzado a rendirse también. Para un hacker esto es bastante fácil. Él o ella necesitan hacer solo más de un requerimiento, rendirse en el entendimiento de uno, luego el objetivo se va a sentir presionado a rendirse en el otro.

La reciprocidad es vista constantemente en el ambiente corporativo. Un empleado ayudará a otro con la expectativa de recibir algo a cambio, eventualmente, el favor será regresado. Este es un sistema cambiante que no está escrito, el mismo que es considerado como invaluable si uno quiere tener éxito. De cualquier manera, la ingeniería social explota este sistema porque los motivos del hacker son deshonestos y él o ella están buscando algo que no debe ser dado a ningún costo.

3.1.6 Relaciones basadas en engaños (Deceptive Relationships)

Otro gatillo psicológico es la construcción de relaciones con el propósito de explotar a otra persona. Una forma de hacer esto es compartir información y discutir sobre un enemigo común. Kevin Mitnick en uno de sus libros indica que su manera favorita de hacer trampas era cuando él estaba tratando con un empleado que ya había sospechado de él en un contexto diferente[16]. Esta vez Mitnick está estableciendo una relación con un empleado a través de un e-mail, compartiendo información y tecnología sin pedir nada a cambio. El también ayudó a vincular la relación hablando negativamente de "Kevin Mitnick" a quien el empleado no culparía por ser el autor de los e-mails. Luego de establecer la relación, Kevin era capaz de obtener toda clase de información sobre el sistema del objetivo.

Una vez que se había desarrollado la relación, hay muchas maneras en las que puede ser explotada. Un buen ejemplo de esto es un ataque a AOL[17], que fue documentado por una revista norteamericana. El hacker llamó y habló con una persona de soporte técnico de AOL por más de una hora. En algún punto durante la llamada el hacker mencionó que su auto estaba de venta. El técnico estaba interesado, entonces el hacker le envió un e-mail con una imagen del auto adjunta. El archivo adjunto contenía un exploit de puerta trasera que abría una conexión aunque AOL tuviera un firewall.

Otra manera en que un hacker puede construir una relación rápida es apareciendo para el objetivo como si ellos fueran muy parecidos. La idea es que la víctima sienta como que él y la persona que está llamando son similares, tienen los mismos intereses o quieren lo mismo en la vida. Creer que alguien tiene las mismas características, idénticas o similares a las nuestras nos da un fuerte incentivo para tratar con esa persona favorablemente hasta confiar en esa persona sin una motivación legítima.

Dentro de esta técnica de ingeniería social podemos encontrar varias maneras en las que una persona puede fingir ser alguien que no es y obtener información.

- Plantearse como un usuario final legítimo:
    - Da su identidad y pide información sensible; por ejemplo:

[16] Mitnick Kevin & Simon William "The art of Deception". Kineticstomp.

[17] America Online, Empresa de servicios de Internet

"Hola, soy Andrés del departamento X, se me olvidó mi clave, ¿podrías dármela por favor?"

- Plantearse como personal de soporte técnico:
  - Llamar como personal de soporte técnico y pedir la identificación y claves de usuario para recuperar información; por ejemplo:

"Señor, soy Cristian de soporte técnico de la compañía X. La noche de ayer tuvimos un problema con el sistema aquí y estamos revisando los datos que se perdieron. ¿Puede por favor darme su nombre de usuario y contraseña para verificar estos datos?"

- Tercera parte autorizada:
  - Se refiere a una persona importante en la empresa que trata de recolectar información:
    - "El señor Pérez, nuestro Gerente Financiero, me pidió que le entregue los reportes de la auditoría financiera, ¿podría usted dármelos para entregárselos a él por favor?"

3.1.7 Difusión de Responsabilidades (Diffusion)

La difusión de responsabilidades se presenta cuando el objetivo hace sentir que él o ella no cargarán solo con la responsabilidad de sus acciones. Irónicamente, este gatillo puede funcionar muy bien con el uso del derecho moral como una motivación para la persuasión. El derecho moral entra al juego cuando el objetivo siente que está haciendo algo para salvar al empleado, para ayudar a la compañía o al menos para evitar sentir culpa.

El blanco siente como que está tomando decisiones que serán la diferencia entre el éxito o el fracaso para la compañía o el empleado que está llamando, implicando que la persona que llama puede perder su trabajo basándose en su decisión. Esta es una decisión muy

difícil de tomar para muchas personas y el empleado cumplirá de manera más fácil si cree que él o ella no poseerán la responsabilidad por esta acción.

3.1.8 Autoridad (Clout)

Las personas están condicionadas a responder ante la autoridad. Un estudio reciente ilustra dramáticamente esta tendencia. Enfermeras en 22 estaciones diferentes de enfermeras fueron invitadas a dar una dosis de un medicamento con prescripción no autorizada a pacientes basadas en órdenes dadas por teléfono (contra la política) de un médico a quien nunca habían conocido y una dosis que era el doble de la dosis diaria. Estas órdenes debían haber sido cuestionadas claramente, todavía en un 95 por ciento de los casos las enfermeras actualmente procuran usar esta dosis y estaban en su camino para administrar el medicamento antes de ser interceptadas por los observadores.

Estos ejemplos dramáticos muestran que la gente va a tener un gran trato con alguien que piensa que es una autoridad. Se podría considerar el impacto que tendría un director o un vice-presidente falso en un empleado que no ha sido preparado. Este gatillo es mucho más poderoso porque en la realidad es un reto verificar la legitimidad de la autoridad, especialmente si se trata de uno de los "jefes". Esta falta de perspectivas deja este gatillo ampliamente abierto para su explotación por cualquiera que esté dispuesto a hacerse pasar por una figura autoritaria.

- Plantearse como un usuario importante:
    - Hacerse pasar por un cliente VIP, una empresa importante, un cliente muy valioso, etc.; por ejemplo:

      "Hola, soy Bárbara, secretaria de la Constructora H&H. Estoy trabajando en un proyecto urgente y perdí mi clave del sistema. ¿Puede ayudarme con eso por favor?"

3.1.9 Integridad y Consistencia (Integrity and Consistency)

Las personas tenemos tendencia a dejarnos llevar por comentarios en el lugar de trabajo aunque estos comentarios no hayan sido muy prudentes.

Para algunos esto es parte de la integridad “hacer lo que uno dice que va a hacer” aunque luego sea sospechoso de que el requerimiento no fue legítimo.

Esta tendencia es tan fuerte que la gente va a llevar a otras personas los comentarios que creen son ciertos y fueron hechos por sus compañeros de trabajo. Si un hacker obtiene un calendario de vacaciones, la ausencia del empleado puede ser explotada usando este gatillo.

Otro aspecto del gatillo de la integridad y consistencia es que la gente tiene la tendencia de creer que otros están expresando sus actitudes verdaderas cuando ellos hacen una afirmación. A menos de que haya una fuerte evidencia de que suceda lo contrario, las personas van a creer que la persona con la que están hablando está diciendo la verdad sobre lo que quiere o necesita. Esta tendencia de creer en otros está basada primeramente en su propia honestidad de expresar sus sentimientos.

3.1.10 Buscar en la Basura (Dumpster Diving)

¿Quién pensaría que botar el correo basura o los documentos de rutina de una compañía sin hacer trizas puede ser una amenaza? Pero esto es exactamente lo que puede ser, si el correo basura contiene identificaciones personales u ofertas de tarjetas de crédito que un

“buscador de basura” pueda usar para llevar a cabo un robo de identidad. El insospechado pica papel puede darle al buscador de basura un descanso.

Las guías telefónicas de la compañía y los mapas de la organización proveen números telefónicos y direcciones de empleados, especialmente niveles administrativos de empleados que pueden ser personificados para el beneficio del hacker.

Los manuales de políticas y procedimientos pueden ayudar al ingeniero social para llegar a tener conocimiento sobre los procedimientos y políticas de la compañía y así ser capaz de convencer a la víctima de su autenticidad.

En su entrevista con la BBC News Online, Kevin Mitnick explica como armarse para un ataque informático con poco conocimiento, un hacker puede simular a un empleado de una firma y conseguir que otros empleados inadvertidamente le suministren una enorme cantidad de información útil.

El hacker puede usar una hoja de papel con el encabezado de la compañía para crear correspondencia que luzca como correspondencia oficial. De la misma forma puede recobrar información confidencial del disco duro, aunque el usuario piense que la información ha sido “borrada” del disco.

La técnica de buscar en la basura es un poco complicada, al momento de obtener información. Esta técnica implica ir a través de las latas o tachos de basura por información o datos sobre la compañía o persona que se ha planteado como objetivo. Al buscar en la basura se puede encontrar desde datos insignificantes hasta la información más confidencial, debido a que muchos empleados piensan una vez que han botado sus papeles en la basura, ellos ya no corren ningún peligro. Mucha gente no piensa en el valor potencial del papel que bota en la basura. Estos documentos usualmente contienen abundante información que le ayuda al ingeniero social a conseguir lo desea o necesita para ingresar en la organización. El ingeniero social que es astuto y con un amplio conocimiento sobre la importancia de la información busca los siguientes documentos impresos:

- Listas de teléfonos internos
- Mapas organizacionales

- Agendas de los empleados, que generalmente contienen las políticas de la organización
- Diagramas de red
- Listas de claves
- Notas de reuniones
- Hojas de cálculo y reportes
- E-mails que contienen información personal

Hacer trizas los documentos en un pica papel es útil cuando el papel es destrozado en trizas pequeñas como las de confeti porque los pica papeles baratos que hacen trizas los documentos en tiras largas son básicos y sin valor contra la ingeniería social. Con poco tiempo y cinta adhesiva, un ingeniero social puede fácilmente reconstruir un documento.

Los hackers también buscan disquetes, CD ROM's y DVD's, partes viejas de computadores (especialmente discos duros) y cintas de respaldo.

3.1.11 Escuchar detrás de las Puertas

Los hackers usualmente obtienen información confidencial personal y de negocios de otras personas escuchando conversaciones en restaurantes, cafeterías y aeropuertos. Las personas que usan un tono alto de voz cuando hablan por el celular son una gran fuente de información. Mientras nos encontramos sin ningún fin malicioso en lugares públicos es increíble lo que se puede escuchar cuando otros están divulgando algo y uno no está tratando de escuchar.

Dentro de esta técnica se encuentra a más de escuchar conversaciones sin autorización, el hecho de leer mensajes que no nos pertenece.

También el interceptar mensajes o conversaciones mediante audio y video es una parte de la técnica escuchar detrás de las puertas.

Actualmente con el avance de la tecnología se puede encontrar en el mercado al alcance de cualquiera de nosotros cámaras de video, cámaras fotográficas e incluso los mismos celulares que ayudan a captar cualquier tipo de información visual o auditiva en cualquier momento y lugar sin que el resto de personas se den cuenta de que se está interviniendo sus actividades o conversaciones.

3.1.12 Mirar sobre el Hombro (Shoulder Surfing)

Otra técnica muy usada por los ingenieros sociales es la llamada shoulder surfing o mirar sobre el hombre, es el acto de mirar a una persona en el teclado de su computadora para detectar y robar su contraseña o la información del usuario.

Es el nombre que se le da al procedimiento que identifica el robo de claves, números de identificación personal, números de cuenta y muchas cosas más.

Simplemente, el atacante mira sobre el hombro del objetivo o puede darse a una larga distancia observando con binoculares, para obtener estos pedazos de información que le serán útiles para llevar acabo su ataque.

Por ejemplo: En la fila que se hace en una entidad bancaria para realizar una transacción en un cajero automático, la persona que está parada detrás de quien está realizando la transacción si no mantiene la distancia adecuada puede fácilmente observar la clave de la tarjeta de esa persona.

3.1.13 Suplantación de Identidad (Impersonation)

Otra metodología muy usada por los ingenieros sociales es la suplantación de identidad, la misma que se puede realizar por varios medios.

3.1.13.1 Llamadas telefónicas

Los hackers pueden obtener información usando el característico marcado por nombre creado en muchos sistemas de correo de voz. Para tener acceso a esta característica, usualmente se presiona la tecla 0 cuando está llamando al número principal de la empresa o a la extensión de alguien en particular. Este truco funciona mejor después de horas en las que no contesta nadie.

Los atacantes pueden protegerse si logran esconder el número telefónico desde el que están llamando. Estas son algunas maneras en las que lo pueden hacer:

- *Teléfonos residenciales:* En varios países los atacantes pueden esconder el número telefónico mediante un código cuando realizan una llamada, pero en Ecuador actualmente no es posible realizarlo, cuando el identificador de llamadas está ya programado para registrar los números, no se lo puede esconder.

- *Teléfonos corporativos:* Los números de teléfono corporativos son más difíciles de imitar en una oficina que usa un switch. De cualquier manera todos los hackers usualmente necesitan la guía de usuario y la clave de administrador para el software del switch del teléfono. En muchos de los switches, el hacker puede ingresar el número fuente (incluyendo un número falso) como el número de la casa de la víctima por ejemplo.

Los hackers encuentran interesantes bits de información, por ejemplo cuando la víctima está fuera de la ciudad, solo escuchando al buzón de mensajes. Ellos también estudian la voz de sus víctimas escuchando los mensajes de voz del contestador, las presentaciones en internet o los Webcasts para personificar a su objetivo.

En esta técnica es muy fácil personificar a alguien más, los ejemplos más claros de esto son los usuarios “nuevos” que han olvidado sus contraseñas, los “jefes” que no recuerdan sus datos y piden una restauración de los mismos, una persona de soporte técnico que necesita sus datos porque tiene algún problema con el sistema o alguien de la mesa de servicios; personas a las cuales por prestarles ayuda les damos información sensible sin haber comprobado antes si en realidad existen o si su identificación es verídica.

3.1.13.2 Ataques internos y empleados descontentos

Un atacante puede tener mucho más éxito conociendo el lenguaje interno y los procesos de negocios. Desplegando conocimiento sobre un proceso interno o procedimiento o usando una jerga interna, el ingeniero social puede engañar al objetivo haciéndole pensar que él o ella es un empleado de su compañía. El hacker puede tener información valiosa sobre el objetivo que se va a atacar; un ex - empleado disgustado esperando para dividir los negocios probablemente conoce a las personas clave que puede usar como peones para el ataque, incluso puede haber establecido algunos cimientos antes de irse; por ejemplo instalar código malicioso. Por este motivo no necesariamente son las personas de afuera las que son más peligrosas, muchas veces podemos encontrar que los mismos empleados o ex – empleados son los que atacan a sus empresas.

Si alguien de la competencia desea causar daño a cierta organización, robar secretos críticos o dejarle a la empresa fuera del negocio, solo debe encontrar una vacante y preparar a alguien para pasar la entrevista, una vez que esté contratado, ya está adentro de la organización, y ya se tiene un cómplice para los ataques.

Es cuestión de encontrar a alguien disgustado que desee tomar revancha y listo, la organización está bajo la mira y bajo un eminente riesgo.

Los ataques más frecuentes en una organización son los de tipo interno con un porcentaje del 82%[18], puesto que ocurren detrás del firewall, son muy fáciles de realizar y son difíciles de prevenir; por el hecho de que el atacante es una persona que está inmersa en la organización y conoce los procesos y procedimientos, lo cual hace más probable que tenga éxito y es más complicado que el agresor sea capturado.

Muchos de estos ataques internos son realizados por individuos introvertidos, incapaces de luchar con el estrés o los conflictos diarios, que están frustrados con su trabajo, con las políticas de la oficina, no sienten respeto, no ha ascendido, etc. Personas que pueden hacerle un gran daño a la empresa, ya que ellos tienen acceso directo a los recursos de la empresa y pueden hacer lo que deseen con ellos, por ejemplo tomar una base de datos y mandársela a alguien de la competencia, el mismo que podría sacar del negocio a la víctima sin mayor problema.

3.1.13.3 Pretexting y engaño mediante palabras o acciones

Pretexting es el acto de crear y usar un escenario inventado (el pretexto) para persuadir al objetivo a liberar información o realizar una acción y es típicamente realizada mediante el teléfono. Es más que una simple mentira, incluye de manera primordial alguna investigación o preparación y el uso de piezas de información conocida (por ejemplo, para la personificación, la fecha de nacimiento, el número de seguro social, el monto de la última cuenta) para establecer legitimidad en la mente de la víctima.

Esta técnica es usualmente utilizada para engañar a un negocio para revelar información de un cliente y es usada por investigadores privados para obtener registros telefónicos, registros de utilidad, registros bancarios y otra información directamente de representantes

[18] http://www.eset-la.com/press/concurso/enemigo-interno.pdf

que proveen servicios en una compañía pequeña. La información puede después ser usada para establecer una mayor legitimidad cuando un gerente haga preguntas (por ejemplo, para hacer cambios en cuentas, obtener balances específicos, etc.).

Muchas compañías en los Estados Unidos para autenticarse todavía le piden al cliente el número de seguro social, la fecha de cumpleaños o el nombre de soltera de su madre; el método todavía es efectivo en varias situaciones pero será un problema de seguridad en el futuro.

Esta técnica puede ser usada también para suplantar a compañeros de trabajo, policía, autoridades bancarias, de impuestos o investigadores de seguros o cualquier otro que pueda percibir autoridad o derecho para convencer a la víctima. El pretexto debe simplemente preparar respuestas a las preguntas que deben ser preguntadas por el objetivo.

Los ingenieros sociales son tan astutos que pueden obtener información de sus víctimas de muchas maneras.

Ellos usualmente están enfocados en mantener sus conversaciones en marcha sin darles a las víctimas mucho tiempo para pensar en lo que ellos les están diciendo. De cualquier modo, si ellos no tienen cuidado o están extremadamente ansiosos sus ataques de ingeniería social pueden traer las siguientes casos que los pueden dejar fuera:

- Actuar demasiado amistoso o ansioso.
- Mencionar nombres de personas destacadas dentro de la organización.
- Alardear sobre la autoridad dentro de la organización.
- Amenazar con reprimendas si los requerimientos que se hacen no son realizados.
- Actuar nervioso cuando se hacen preguntas (fruncir los labios y estar inquietos, especialmente con las manos y los pies porque se requiere de un mayor esfuerzo para controlar partes del cuerpo que estaban lejos de los pies).
- Sobre enfatizar en los detalles.
- Cambiar sicológicamente, tener las pupilas dilatadas o cambios en el tono de voz.
- Aparecer apresuradamente.
- Refutar al dar información.
- Dar información voluntariamente y responder preguntas que no han sido planteadas.

- Conocer información que una persona ajena no debe tener.
- Un intruso conocido usando discursos o jergas internas.
- Preguntar cosas extrañas.
- Escribir mal algunas palabras en comunicaciones escritas.

Un buen ingeniero social no es obvio con las acciones que realiza pero estas son varias de las señales que tiene un humano en el comportamiento malicioso dentro del trabajo.

Los hackers usualmente le hacen un favor a alguien y luego regresan hacia esa persona y le piden que haga algo por ellos. Este es un truco común en la ingeniería social que funciona muy bien. Aquí es donde ellos ofrecen ayuda en problemas específicos que surgen; algún tiempo pasa, el problema ocurre (generalmente porque ellos lo ocasionan) y luego ellos solucionan el problema. Ellos vienen como héroes, lo que puede elevar más allá su causa. Los hackers también pueden pedir un favor a un empleado que no sospecha de ellos.

Personificar a un empleado es fácil. Un ingeniero social puede vestir de manera similar el uniforme, hacer una credencial falsa o simplemente vestir como los empleados reales. Ellos generalmente se hacen pasar por empleados. La gente piensa “Oye, el luce y actúa como yo, entonces el debe ser uno de nosotros.” Los ingenieros sociales también pretenden ser empleados llamando desde fuera y dentro por teléfono. Esta es especialmente una manera de explotar al personal de la mesa de ayuda y del call center. Los atacantes saben que es fácil que estas personas caigan en una rutina debido a la repetitividad con la que dicen, “Hola, ¿puede ayudarme con su número de cliente, por favor?”

Un ejemplo de este tipo de ingeniería social; es acerca de una mujer que no pensó bien antes de responder y fue atacada mediante ingeniería social. Un día tenía problemas con la conexión de Internet, a lo que supuso, que solo podía usar acceso dial-up porque es mejor que nada para acceder al e-mail y otras tareas básicas. Ella contactó a su ISP y le dijo al muchacho de soporte técnico que no recordaba su contraseña dial-up. Esto suena como el comienzo de un ataque de ingeniería social que ella pudo haber detenido pero siguió con él. El astuto muchacho de servicio técnico hizo una pequeña pausa, como si estuviera buscando la información de esa cuenta y luego le preguntó, “¿Con qué clave trató?” Estúpidamente ella le dio todas las claves que ella podía usar. El teléfono estuvo callado por un momento, el re-configuró la contraseña y le dijo cual era. Después de que ella colgó

el teléfono pensó, “¿Qué acaba de pasar?” Había sido víctima de un ataque de ingeniería social. Ella estaba muy molesta consigo misma, tuvo que cambiar todas las contraseñas que había divulgado en caso de que el hombre del ISP usará esa información en contra de ella. Lo que ella pensó es que él estaba experimentando con ese ataque y aprendió la lección: Nunca, jamás bajo ninguna circunstancia divulgará las contraseñas a nadie más.

3.1.13.4 Obtener acceso físico (Tailgating & Piggybacking)

Muchos oficiales corporativos tienen mucha información asequible que puede ayudar a un ingeniero social a perpetrar su ataque. A pesar de que los ingenieros sociales tienden a evitar el sitio de un objetivo, hacerlo puede ser fácil. En estos días, las organizaciones más grandes usan sistemas de insignias para entrar en un edificio o área segura. Estos seres humanos generalmente son corteses, seguir a alguien en un ambiente corporativo puede ser muy simple. En las organizaciones grandes muchos empleados no conocen a cada empleado o reconocen cada cara y son usualmente más que felices por sostener la puerta para alguien más. Una vez adentro, el ingeniero social puede obtener buena información solo caminando por los espacios de trabajo de los empleados que están caminando lejos. Si camina a través de las oficinas, el ingeniero social puede encontrar claves en papeles pega-despega (post it) en monitores, registros financieros como facturas y órdenes de compra o documentación en la infraestructura técnica. El atacante puede salir de la oficina con información en las manos.

Estar en este lugar trae más ventajas después de horas. Los ingenieros sociales se hacen pasar por trabajadores de limpieza o mantenimiento después de algún tiempo; incluso algunos pueden buscar una compañía de trabajos y pedir que los coloquen como personal de limpieza en la compañía del objetivo. Una vez adentro pueden encontrar estaciones de trabajo que no hayan bloqueado o cerrado la sesión e instalar software malicioso o robar información.

El hacker puede encontrar información sensible que no fue destruida apropiadamente; él o ella, puede instalar equipos de red como Access points de redes wireless o inalámbricas. Un ingeniero social que entra en la empresa del objetivo va a ser tan rápido y cauteloso como le sea posible, pero en la noche cuando nadie está cerca él o ella puede bajar la guardia un poco más y tomar más tiempo recolectando información. Un ingeniero social que no ha sido detectado en la oficina después de varias horas puede fácilmente robar hardware y software o cualquier otra cosa que le pueda ser útil para alcanzar su meta.

3.2.INGENIERÍA SOCIAL BASADA EN COMPUTADORES

La ingeniería social basada en computadores es aquella que se lleva a cabo con la ayuda de computadoras o elementos tecnológicos, con los cuales se logra que el usuario crea que está interactuando con el sistema computarizado real y se puede obtener información confidencial a través de estos medios. Por ejemplo, el usuario encuentra una ventana emergente, informándole que su aplicación tiene un problema y que el usuario va a tener que autenticarse de nuevo para poder continuar. Una vez que el usuario haya ingresado su usuario y su clave en la ventana emergente, el daño está hecho. El hacker que ha creado el Pop-Up ahora tiene el identificador o usuario y la clave y puede tener acceso a la red y al sistema computacional.

La ingeniería social basada en computadores puede ser dividida en las siguientes categorías:

- Correo / Enlace IM
- Windows Pop – Up
- Sitios web / Loterías
- Correo basura
- Phishing

Windows Pop – Up:

En Windows repentinamente se abren los Pop – Up o ventanas emergentes mientras navegamos en Internet, nos preguntan sobre información de usuario, para registrarnos o entrar en algún lugar.

Cartas de engaños o cadenas:

- Las cartas con engaños son correos electrónicos que emiten avisos al usuario sobre nuevos virus, troyanos o gusanos que pueden dañar el sistema del usuario.
- Las cartas con cadenas son correos electrónicos que ofrecen regalos gratuitos como dinero o software si el usuario reenvía el correo a determinado número de personas

Mensajería de conversación instantánea:

- Conseguir información personal mediante el chat sobre un usuario seleccionado previamente, datos como fechas de cumpleaños, nombres de soltero, etc.
- Adquirir datos para craquear[19] cuentas de usuario.

Correo basura:

- Correos electrónicos enviados a muchas personas simultáneamente sin autorización previa con fines comerciales.
- Correos electrónicos irrelevantes, no deseados y no solicitados para recolectar información financiera, números de seguro social e información de red.

E-mails e Internet

En esta metodología el objetivo participa involuntariamente. Hay dos formas en que esta es usada actualmente:

- La primera implica que en un e-mail se adjunta código malicioso, por ejemplo el que se usa para crear un virus. Este código usualmente es escondido dentro de un archivo adjunto en el correo electrónico.
- La intención es que el usuario no sospeche y abra el archivo. Y la segunda forma igualmente efectiva envuelve una cadena de correos y virus en cartas de engaño; estos han sido diseñados para obstruir el sistema de correo reportando un virus no

[19] Craquear: Usar un programa que modifica de forma temporal o permanente una aplicación para eliminar limitaciones o candados impuestos en los mismos originalmente.

existente o competencias y peticiones al destinatario para reenviar una copia a todos sus amigos y compañeros de trabajo. Como nos ha mostrado la historia esto puede crear un efecto de “bola de nieve” gigante una vez que ha comenzado.

Estos ataques pueden llevarse a cabo copiando la identidad de la compañía por ejemplo y enviando un mail como si el atacante fuera parte de la misma y le decimos que ingrese a X sitio web para activar el proceso de actualización de información personal por motivos de seguridad o le pedimos su identificación del sistema, etc., esto se logra haciendo que el mail parezca legítimo y real (tipos de letra, colores, logotipo de la compañía, etc.).

Al igual que con el uso del correo electrónico los ingenieros sociales pueden hacer uso del correo tradicional también; de la misma manera toman logos de ciertas empresas y ya conociendo varios datos pueden encaminar el ataque, por ejemplo dicen que son de una tarjeta de crédito X y que debido al monto que han comprado en determinado tiempo han sido acreedores a un viaje con todos los gastos pagados pero que deben enviar una contestación confirmando sus datos y que les enviarán los pasajes o algo por el estilo, de esta manera el objetivo va a dar la información que se requiera de manera muy fácil y sin poner ninguna objeción.

Aparte de los e-mails se pueden realizar ataques vía internet ya que hoy en día el internet es una herramienta básica en las investigaciones o búsquedas que se realizan a diario. Unos pocos minutos en Google o cualquier otro buscador, usando palabras claves como el nombre de la compañía o nombres de empleados específicos nos va a dar como resultado una gran cantidad de información. Muchas organizaciones (especialmente con cargos altos) pueden asustarse con toda la información que está disponible. Usando estos buscadores y yendo directamente al sitio web de la compañía, el atacante puede encontrar suficiente información para comenzar.

Los hackers pagan $100 o menos por los antecedentes comprensibles de los individuos que van a atacar. Estas búsquedas pueden llevarse a cabo prácticamente con cualquier información pública y algunas veces privada de ciertas personas en minutos.

Phishing

El llamado phishing es otra técnica de la ingeniería social, es una forma de robar identidades en el que un tramposo usa un buscador de identidades de e-mail para engañar a

los destinatarios para recibir información personal sensible, tal como, número de tarjeta de crédito, cuantas bancarias o número de seguro social.

Los ataques que se realizan mediante phishing usan tanto ingeniería social como técnicas de excusas para robar datos de identificación personal de los clientes y credenciales de cuentas financieras.

Podemos encontrar para mitigar este tipo de ataques el ejemplo de "Yahoo añade escudos anti-phishing" en el que Yahoo está probando una nueva característica de seguridad que le permite al usuario personalizar su página de ingreso, una medida diseñada para estorbar a los ladrones de identidades usando phishing. Esta característica requiere que la gente cree una señal única en una computadora específica. Este sello (un mensaje de texto o una foto) será desplegada en la página de inicio de Yahoo cuando se visite esta página desde esa computadora, de acuerdo a la descripción en esta característica del sitio web de Yahoo.

Hoy en día los ataques que se llevan a cabo mediante phishing son los más comunes en el robo de identidad corporativo; este envuelve usualmente un mensaje de e-mail pidiéndole al consumidor que actualice su información personal con un vínculo a un sitio Web imitado.

Actualmente es bastante fácil crear sitios Web que parezcan auténticos para poder robar la identidad o información de las personas; los atacantes que realizan fraudes comúnmente atacan a corporaciones conocidas para robar sus identidades, el nombre de sus productos y sus logotipos.

Podemos encontrar muchos ejemplos de esto ya que los atacantes usan nombres conocidos y sus páginas, por ejemplo: PayPal, MSN y Visa; fingiendo ser ellos, mandan e-mails o crean páginas para ingresar en sus cuentas y es ahí cuando roban la información de la víctima; envían esta información a otra dirección URL y la víctima al no ver la barra en la que se despliega la dirección o simplemente al no saber cuál es la dirección original a la que se direcciona esta página no se da cuenta de que esto está sucediendo.

Dentro del phishing se puede encontrar los marcos o frames escondidos con los cuales los atacantes toman nuestros datos, esto se ha vuelto muy popular para esconder contenido de ataque; tienen soporte semejante para todos los exploradores y un estilo de fácil codificación. El atacante debe sólo definir código HTML usando dos marcos; el primer

marco contiene la información del sitio URL legítimo mientras que el segundo marco 0% de la interface del explorador y está corriendo código malicioso en el mismo.

Dentro de este tipo de métodos de ataque encontramos la ofuscación URL, la que usa cadenas de código o texto en la dirección URL, usa signos que son reconocidos como válidos como el signo @ que es muy usado en varios sitios para autenticarse. Esto sucede también cuando la dirección a la que queremos acceder es demasiado larga, de manera que no se muestra por completo en la pantalla y ahí se esconde la parte maliciosa o simplemente se usan nombres similares en las direcciones URL a las que deseamos acceder.

Dentro del phishing podemos encontrar barra de direcciones, barras de herramientas y barras de estado falsas que le ayudan al hacker a obtener la información que desea.

Spear phishing o Ataques dirigidos que parecen proceder de personas conocidas:

En la categoría de "spear phishing" se incluye cualquier estafa de correo electrónico dirigida a un objetivo específico y que suele aparecer en un entorno empresarial.

Los timadores de "spear phishing" envían mensajes de correo electrónico que parecen auténticos a todos los empleados o miembros de una determinada empresa, organismo, organización o grupo.

El mensaje puede parecer procedente de un compañero de trabajo o de un responsable (como el jefe de recursos humanos o de TI), que podría enviar un mensaje de correo electrónico a todos los usuarios de la empresa. Podría incluir solicitudes de nombres de usuario y contraseñas o contener software malintencionado, como un troyano o un virus.

La estafa de "spear phishing" corresponde a un tipo de ingeniería social más avanzado que el "phishing", pero las técnicas que pueden usarse para evitar ser engañados son las mismas.

Cuadro de resumen de las técnicas más usadas de ingeniería social:

A continuación se encuentra un cuadro en el que se encuentran las técnicas de ingeniería social en su área de riesgo y la estrategia con la que se combaten

Área de Riesgo	Táctica	Estrategia de Combate
Teléfono (Mesa de Ayuda)	Personificación y persuasión	Entrenar a los empleados y mesa de ayuda a nunca dar contraseñas u otra información confidencial por teléfono.
Teléfono (Mesa de Ayuda)	Personificación en las llamadas de la mesa de ayuda	Todos los empleados deben tener asignado in PIN específico para ayudar al personal de la mesa de soporte.
Teléfono y PBX	Robar acceso telefónico	Controlar llamas de larga distancia y extranjeros, rastrear las llamadas, negar transferencias
Construir una entrada	Acceso físico no autorizado	Señal cerrada de seguridad, entrenamiento de empleados y presentación de los oficiales de seguridad.
Oficina	Mirar sobre el hombro	No escribir contraseñas con alguien presente (y si debe hacerlo, hacerlo de manera rápida)
Oficina	Vagar a través de pasillos buscando puertas abiertas	Requerir que todos los empleados sean escoltados
Oficina	Robo de documentos sensibles	Marcar documentos como confidenciales y requerir que estos documentos estén cerrados.
Habitación de correo	Inserción de memos falsificados	Cerrar y monitorear la habitación de correo.
Cuarto de	Tratar de obtener acceso,	Mantener cerrados los

máquinas/armario de teléfono	quitar equipo, y/o adjuntar un analizador de protocolos para aprovecharse de los datos confidenciales	armarios de teléfono, cuartos de servidores, etc., todo el tiempo y mantener actualizado el inventario de equipos.
Basureros	Buscar en la basura	Mantener todos los basureros seguros, monitorear las áreas, triturar todos los documentos importantes, borrar los medios magnéticos.
Intranet - Internet	Creación e inserción de software ficticio en la intranet para capturar contraseñas	Continua concienciación de los cambios del sistema y de la red, entrenamiento del uso de contraseñas.
General - Sicológico	Personificación y persuasión	Mantener a los empleados alerta a través de concienciación continua y programas de entrenamiento.

Tabla 3.1: Estrategias de combate por área de riesgo

CAPITULO IV

4. ATACANTES Y ESTRUCTURA DE UN ATAQUE

Como parte de la ingeniería social es importante estudiar el comportamiento humano debido a que las personas que llevan a cabo ataques con esta técnica, es decir, los ingenieros sociales, siguen un patrón de comportamiento como todos los criminales en los diversos ámbitos en los que pueden atacar.

Los ingenieros sociales pueden ser relacionados con los criminales que actúan en otros ámbitos, por ejemplo: los asesinos, los ladrones, los estafadores, etc.; debido a que ellos tienen características comunes mediante las cuales pueden ser identificados, así también los ingenieros sociales, es decir, siguen un patrón para cometer sus actos ilícitos, por lo que es importante saber qué es un perfil criminal y cómo se perfila a uno.

4.1. PERFIL DE UN CRIMINAL

Como ya habíamos visto podemos encontrar diferentes tipos de ingenieros sociales, los mismos que pueden tener diferentes características, de entre las que podemos resaltar como las más notorias e importantes a las siguientes:

- Tienen una personalidad muy introvertida.
- Son buenos programadores.
- Pasan mucho tiempo solos, pensando cual va a ser su siguiente movimiento para el ataque.
- Son personas que tienen deseos de ser conocidas o que quieren simplemente demostrar que pudieron hacer un ataque en un lugar seguro

- Son empleados que no están contentos, que prefieren ganar dinero de una manera más fácil o prestigio ante los demás empleados.
- Son jóvenes con mentes abiertas que simplemente realizan sus ataques por curiosidad.
- Personas que se dejan influenciar por hackers conocidos y comienzan haciendo pequeños trabajos para un hacker prestigioso para ganarse su confianza y poder llegar a ser como él (ella).

Estas son características típicas entre los hackers o ingenieros sociales, una vez que las hemos encontrado podemos crear un perfil del atacante, por lo que en este subcapítulo hablaremos sobre el perfil de un criminal, describiremos qué es y un poco de la historia sobre como empezaron a perfilarse los criminales, porqué y para qué.

4.2. QUÉ ES UN PERFIL CRIMINAL

Para una gran mayoría de gente, un perfil criminal consiste en información que sirve predominantemente para describir las características biográficas de los posibles perpetradores de un crimen. Entonces, los perfiles criminales típicamente contienen información sobre el posible agresor teniendo en cuenta lo siguiente:

- Características demográficas, como edad o género.
- Historia legal, incluyendo cualquier antecedente (por ejemplo historial de ofensas criminales prioritarias)
- Formación vocacional (por ejemplo el trabajo en el que el agresor está inmerso, si hubiera alguno)
- Características familiares (por ejemplo la formación de la familia del agresor)
- Hábitos e intereses sociales (deportes, hobbies u otros intereses que el agresor pueda tener)
- Modo de transportarse (tipo de vehículo, si el agresor tuviera alguno)
- Varias características de la personalidad del individuo (la conducta del agresor, apariencia, etc.)

Adicional a esta información, se debe notar que los perfiles criminales incluyen también frecuentemente información perteneciente a la ubicación aproximada de la residencia del criminal.

Al describir la aplicación de perfiles criminales, se debe enfatizar que contrario a muchas descripciones ficticias, los perfiles criminales por ellos mismos no resuelven ningún crimen. En su lugar, perfilar criminales es bien visto como una fuente que puede ser usada para ayudar en investigaciones criminales cuando los métodos convencionales que se emplean han fallado al identificar al perpetrador.

4.3. ESTRUCTURA DE UN ATAQUE

Hay un patrón común asociado con los ataques de ingeniería social; el mismo que es evidente, es reconocible y prevenible.

Este patrón puede ser conocido como el ciclo del ataque o como la estructura que tiene un ataque y consiste en cuatro fases:

1. Obtener información sobre el objetivo o blanco
2. Desarrollar una relación con el objetivo o blanco
3. Explotar la relación que se formó previamente con el objetivo o blanco
4. Ejecutar los planes que tenía el atacante

Cada ataque de ingeniería social es único, con la posibilidad de que este puede envolver múltiples ciclos o fases y/o puede incorporar el uso de otras técnicas tradicionales que se utilizan en otros ataques para conseguir el resultado deseado.

A continuación se describirán más a fondo las fases o etapas por las que pasa un ataque de ingeniería social.

4.3.1 Obtener Información sobre el objetivo

El primer paso en la estructura de un ataque de ingeniería social es obtener información sobre el objetivo o blanco al que se desea atacar; para conseguir esta información pueden ser usadas una variedad de técnicas. Una vez que se ha obtenido o recolectado la información se puede construir una relación basada en estos datos, lo que hace suponer que esta relación será exitosa.

Anteriormente ya hemos mencionado técnicas que usan los ingenieros sociales para recolectar información, las mismas que son usadas en este punto del ciclo de la ingeniería social; por ejemplo se puede usar el método de escarbar en la basura, parece una técnica que no es muy útil o que no va a dar los resultados que esperamos pero en realidad es una técnica que se usa a menudo y que nos puede dar mejores resultados de los que podemos pensar; de esta manera podemos encontrar listas de números telefónicos, fechas de cumpleaños, fechas de reuniones, agendas, direcciones, puestos de trabajo, etc., información que va a ser muy importante y de mucha utilidad al momento de entablar una conversación con el objetivo para pasar al siguiente paso de formar una relación.

Otra de las técnicas que podemos encontrar para recolectar información es usando mails falsos o suplantando la identidad de alguien, por ejemplo si enviamos un e-mail figurando ser de la tarjeta de crédito X y le decimos que necesitamos que actualice su información y en medio de estos datos le preguntamos por cosas que le gustan, por sus preferencias, por sus hobbies, etc., vamos también a obtener información que nos va a ayudar a conocer mejor al blanco y va a ser más fácil comenzar una relación con dicha persona ya que sabemos lo que le gusta y lo que quiere.

4.3.2 Desarrollar una relación con el objetivo o blanco

El atacante después de haber obtenido toda la información que pudo sobre el objetivo blanco debe clasificar esta información y saber como usarla, una vez que conoce los gustos y necesidades del blanco o pequeños detalles como el día de su cumpleaños, si tiene familia, etc., debe aprovechar todas estas cosas para acercarse a él y entablar una relación con él o ella. Mientras va entablando esta relación y ganando la confianza del objetivo se pone en una posición privilegiada que después le servirá para conseguir lo que está buscando.

Por ejemplo el ingeniero social buscó en la basura y encontró un listado de los e-mails de la empresa y con esto le envió un correo electrónico a su objetivo, le preguntaba qué deporte practica, cuántas veces al mes lo hace, qué le gusta, con quién practica este deporte, etc. De manera que el atacante sabe algo que es importante en la vida de la víctima. Una vez que conoce esto, va a acercarse personalmente a su blanco y usando la información que había obtenido mediante el e-mail va a entablar una conversación con su objetivo y poco a poco va a ir ganándose su confianza para así tener una relación cercana con él o ella.

4.3.3 Explotar la relación

Después de haber creado una relación con el objetivo y haber ganado su confianza, el objetivo puede ser manipulado a gusto del atacante, como ahora no es un peligro para él sino al contrario es una persona en la que confía, a la que le puede revelar información confidencial o ejecutar una acción que no haría por cualquier persona; por ejemplo revelarle su nombre de usuario o prestarle su contraseña. Esta fase puede ser el fin del ataque o el comienzo de la siguiente fase.

CAPITULO V

5. HERRAMIENTAS MAS COMUNES PARA MITIGAR LOS ATAQUES MEDIANTE INGENIERIA SOCIAL

Cuando se habla de herramientas de ingeniería social, se encuentran herramientas tecnológicas, las cuales son usadas contra los ataques realizados mediante phishing; de igual forma se pueden encontrar herramientas contra los ataques que se llevan a cabo con las técnicas basadas en humanos, estas herramientas son las políticas de seguridad.
A continuación serán descritas algunas herramientas conocidas para los ataques realizados mediante phishing.

5.1. NETCRAFT

La herramienta Netcraft contiene elementos que pueden indicar indicios de fraude en el sitio web visitado.

Por ejemplo, muestra la popularidad del sitio entre los usuarios (cuanto más visitado, más de fiar), el país donde se aloja el sitio y un índice de riesgo calculado por la propia barra de herramientas.

Se caracteriza por:

- Proteger de los ataques de phishing.
- Vigilar donde se hospeda y proporciona un índice de riesgo de los sitios que han sido visitados.
- Ayudar a defender a la comunidad internauta de fraudes.

La forma de proceder de la herramienta es que cada vez que se informa sobre un mail de phishing se consigue la URL destino a la que se envía la información, y está es bloqueada para la comunidad de miembros. Y dado que en los casos de phishing se envían cantidades masivas de correo, y es relativamente fácil identificarlos, se descubrirán rápidamente y se producirá el bloqueo de la URL correspondiente.

Para una gran mayoría de gente, un perfil criminal consiste en información que sirve predominantemente para describir las características biográficas de los posibles perpetradores de un crimen. Entonces, los perfiles criminales típicamente contienen información sobre el posible agresor teniendo en cuenta lo siguiente:

- Características demográficas, como edad o género.
- Historia legal, incluyendo cualquier antecedente (por ejemplo historial de ofensas criminales prioritarias)
- Formación vocacional (por ejemplo el trabajo en el que el agresor está inmerso, si hubiera alguno)
- Características familiares (por ejemplo la formación de la familia del agresor)
- Hábitos e intereses sociales (deportes, hobbies u otros intereses que el agresor pueda tener)
- Modo de transportarse (tipo de vehículo, si el agresor tuviera alguno)
- Varias características de la personalidad del individuo (la conducta del agresor, apariencia, etc.)

Adicional a esta información, se debe notar que los perfiles criminales incluyen también frecuentemente información perteneciente a la ubicación aproximada de la residencia del criminal.

Al describir la aplicación de perfiles criminales, se debe enfatizar que contrario a muchas descripciones ficticias, los perfiles criminales por ellos mismos no resuelven ningún crimen. En su lugar, perfilar criminales es bien visto como una fuente que puede ser usada para ayudar en investigaciones criminales cuando los métodos convencionales que se emplean han fallado al identificar al perpetrador.

Esta herramienta tiene un licenciamiento libre, es decir, se descarga libremente desde Internet y no tiene un costo, simplemente se deben seguir los términos y condiciones de uso para poder usarlo.

El porcentaje de uso de esta herramienta, se divide según los países en los que más se utiliza, esto se puede observar en la siguiente tabla:

PORCENTAJE	PAIS
56	Estados Unidos
6	Reino Unido
4	Alemania, Canadá
2	Japón, Holanda, Francia, Suecia, Italia
2	Desconocido
1	Suiza, Australia, Korea, India
12	Resto del mundo

Tabla 5.1: Porcentaje de uso de Netcraft

El logo mediante el cual puede ser reconocido Netcraft y su barra anti-phishing es el siguiente:

5.2. EARTHLINK

La herramienta Earthlink es una barra de herramientas que califica según sus propios criterios los webs visitados como 'Seguro', 'Sospechoso' o 'Fraudulento'. En este último caso, se bloquea el acceso a dicho web.

Existe un cuarto estado ('Neutral') que no garantiza que sea un sitio seguro, pero no tiene motivos para sospechar de él.

Dentro de las características de esta herramienta se encuentra el bloqueo de ventanas emergentes.

La licencia de esta herramienta es gratuita, por lo que simplemente se la descarga del Internet y se la instala.

El logotipo con el que se puede reconocer a esta herramienta es el siguiente:

5.3. GEOTRUST

La herramienta Geotrust indica la fiabilidad del web visitado mediante un código de colores (rojo - amarillo - verde).

La fiabilidad de un sitio depende de si su validez ha sido o no comprobada por los autores de la barra.

Indicador de Estado

VERIFIED

El sitio está verificado y es seguro el uso de información personal y confidencial.

NOT VERIFIED

El sitio no está verificado. No tiene porque se malo, simplemente no **TrustWatch** no lo ha verificado.

WARNING

El sitio visitado es fraudulento.

Dentro de las características de este sitio se encuentran:

- Informar sobre un fraude
- Bloquear ventanas emergentes
- Enseñar el sitio web real que se está visitando

La licencia de este producto tiene un costo de alrededor de 80 euros, la misma que nos garantiza que esta herramienta envía certificados de autenticación del sitio web del que estamos recibiendo la información.

El logotipo con el cual se puede reconocer a esta herramienta es el siguiente:

Existen herramientas o software que sirve para controlar la fuga de información a través de correo electrónico, dispositivos de almacenamiento, impresiones, etc., dentro de estas se puede encontrar algunas.

5.4. WEBSENSE CONTENT PROTECTION SUITE

Combina la concienciación de contenido y contexto apoyando la inteligencia Web a través de la integración con la base de datos de URLs de Websense y la tecnología de clasificación de contenido malicioso ThreatSeeke, así como nuevas capacidades de reconocimiento de información basadas en el contexto que incrementan la precisión de la

detección y permiten a las organizaciones crear y hacer cumplir políticas de compartición de información y de usuario específico.

Dentro de las características que se pueden encontrar dentro de esta herramienta se encuentran las siguientes:

- Conocimiento y control del contexto
- Conocimiento mejorado del contenido
- Protección de seguridad avanzada
- Mejoras en administración y despliegue

La licencia de este software o herramienta tiene un costo, como la mayoría de programas cuenta con una versión de prueba.

La imagen con la que se puede reconocer a esta herramienta, es la siguiente:

5.5. SYMANTEC DATA LOSS PREVENTION

Symantec Data Loss Prevention ofrece una solución unificada para detectar, supervisar y proteger la información confidencial sin importar dónde se almacene o cómo se utilice. Symantec ofrece cobertura completa de los datos confidenciales en sistemas de almacenamiento, endpoints y redes. Al reducir notablemente los riesgos, verá su confianza renovada para demostrar el cumplimiento mientras protege la imagen de la empresa, la propiedad intelectual y los clientes.

Dentro de las funciones principales de esta herramienta podemos encontrar:

- Detección: Localiza la información confidencial
- Supervisión: Comprenda de qué modo se usa la información confidencial
- Protección: Aplicar políticas de seguridad automáticamente
- Administración: Definir políticas universales para toda la empresa

Esta herramienta dispone de una licencia pagada para diversos tipos de empresas, con diferentes tipos de acuerdos y en ciertos casos se pueden encontrar descuentos.

El logotipo con el que se puede distinguir este software es:

5.6. MCAFEE

La empresa McAfee, presenta varias alternativas en cuanto a software y hardware se refiere para controlar la fuga de datos, a continuación se indican los nombres de las mismas:

- McAfee Device Control: Regula el uso de medios portátiles en la red
- McAfee Host Data Loss Prevention: Supervisa y controla la manera en que los empleados transfieren datos de negocio.
- McAfee Network DLP Discover: Identifica y protege los datos delicados.
- McAfee Network DLP Manager: Usa dispositivos a lo largo de la red para controlar la pérdida de datos.
- McAfee Network DLP Monitor: Crea reglas complejas, mediante las cuales controla los datos que son enviados.
- McAfee Network DLP Prevent: Aplica políticas para proteger los datos que están en movimiento.
- McAfee Port Control: Controla el uso de dispositivos portátiles conectados en la red.

Todas estas herramientas, ya sean software o hardware, cuentan con una licencia pagada, la cual depende de la herramienta de la que se trata.

El logotipo con el cual se reconocen estas herramientas es:

CAPITULO VI

6. CASO PRÁCTICO

6.1. INSERCIÓN DE UN KEYLOGGER PARA OBTENER INFORMACIÓN CONFIDENCIAL

Como parte del tema de estudio, se realizó un ataque de ingeniería social a una empresa de nuestro país, para analizar cuál es la manera de realizar un ataque, los pasos que se siguen, las herramientas que se utilizan, los métodos a través de los cuales se puede atacar; a continuación son descritos los pasos que realizaron y las herramientas que se usaron para alcanzar el objetivo.

Los pasos que se siguieron para realizar este ataque fueron:

- Se busca un servidor FTP.
- Se busca un keylogger que cumpla con el objetivo planteado y pueda enviar los logs guardados de alguna manera, en este caso vía FTP.
- Se configura el keylogger y se crea el instalador.
- Se genera un solo archivo, entre el keylogger y una imagen cualquiera para enviárselo a la víctima.
- Se cambia la imagen del archivo para que no sea sospechoso.
- Se guarda este archivo en un cd.
- Se crea una carta con una excusa convincente hacia la víctima para que use el cd y se ejecute el keylogger.
- Se reciben y revisan los logs generados.

Todos estos pasos se describen a detalle en las siguientes páginas.

Lo primero que se debe hacer es buscar un servidor FTP; actualmente existen varios en la Web, para este caso se utilizó el servidor drivehq.com; en este lugar, se llenan los datos

para completar el registro, como se realiza para crear un correo gratuito o una suscripción cualquiera. Una vez creada la cuenta, se puede encontrar varias carpetas, en las que se puede compartir toda clase de información.

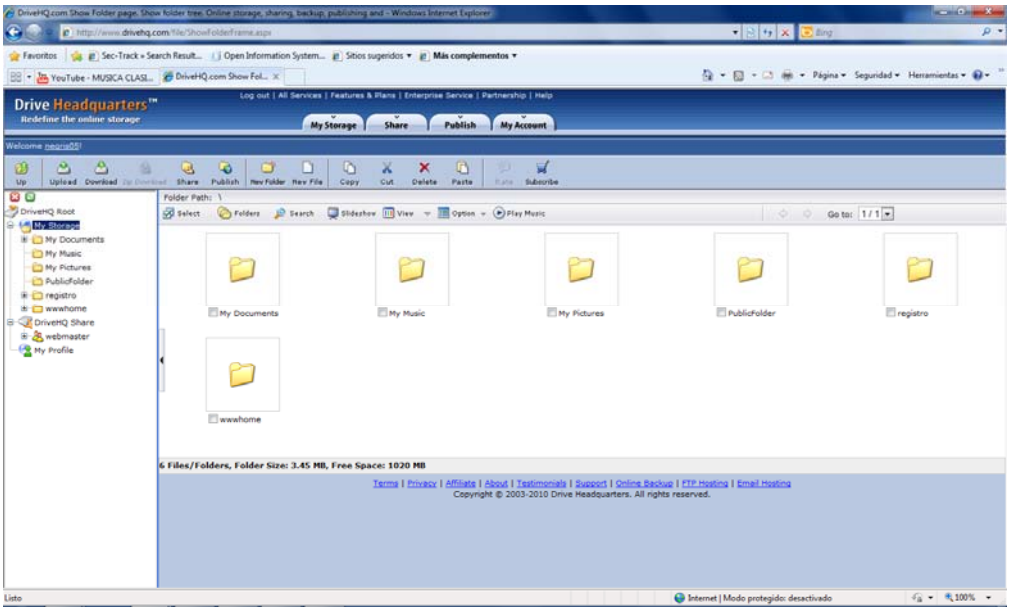


Figura 6.1 Servidor FTP

Con el fin de manejar de una manera más fácil y ordenada los logs que se van a generar con el keylogger, se creó una carpeta “registro”, lugar en el cual se guardarán los archivos enviados remotamente.

Después de haber creado la cuenta en el servidor FTP, se descarga un keylogger que pueda administrarse de manera remota, en este caso se utilizó el Ardamax 2.8; una vez descargado se lo instala en la máquina en la que se va a crear el instalador para la víctima; la instalación del mismo se realiza a través de un wizard como cualquier programa.

Una vez instalada o configurada la herramienta, se registra el programa con la clave y el usuario que viene cuando realizamos la descarga; en caso de no realizar este registro no se lo podrá usar de manera remota.

Cuando está registrado el keylogger, se procede a configurar el instalador que actúa de manera remota, se hace de la siguiente manera:

1. Click derecho en el ícono de Ardamax y se escoge la opción de Remote Installation o Instalación Remota, la primera pantalla que aparece es la bienvenida, en la que se explica que este wizard crea un paquete de instalación personalizado; éste da como resultado un archivo ejecutable con todos los archivos necesarios incluidos e indica que este paquete o instalador puede ser enviado por e-mail una vez que se ha completado el wizard y cuando alguien presione doble click sobre este se instalará automáticamente.

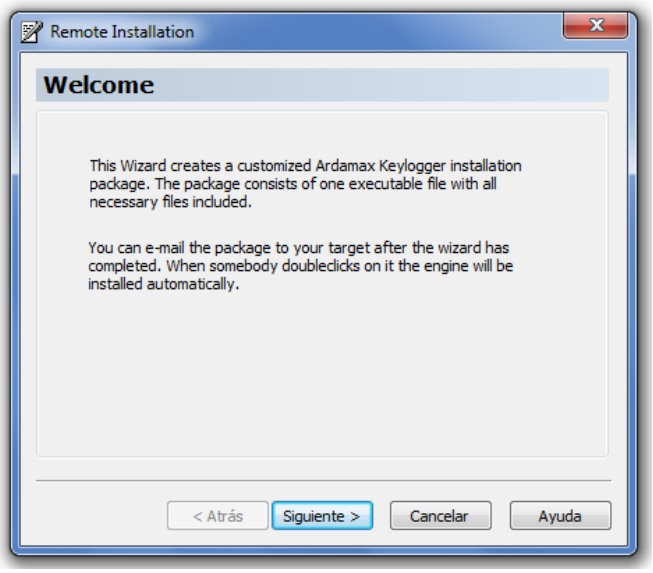


Figura 6.2. Inicio de instalación Ardamax

2. La siguiente pantalla muestra en la carpeta en la que se instalará el keylogger y se puede escoger si se desea componentes adicionales, sin embargo, es mejor no escoger ningún componente adicional para que el keylogger tenga mejor efectividad y no sea detectado.

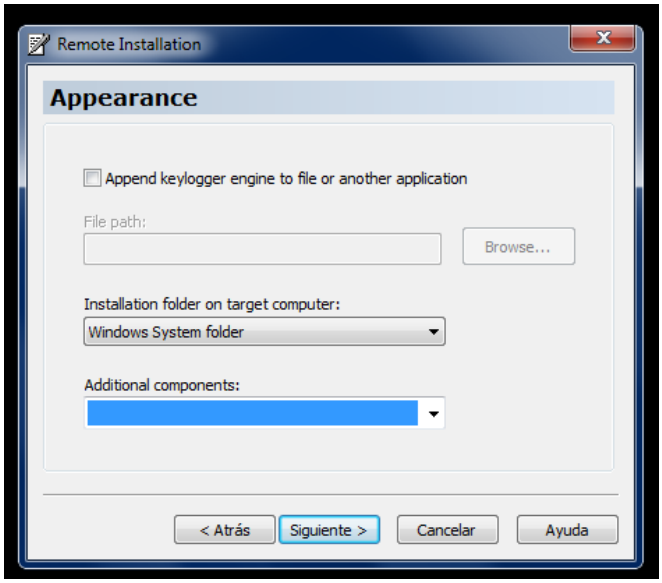


Figura 6.3. Carpeta de instalación de keylogger

3. En la tercera pantalla se puede escoger las opciones de invisibilidad con las que se desea instalar el keylogger; lo óptimo es poner un check en todas las opciones para que sea completamente invisible e indetectable.

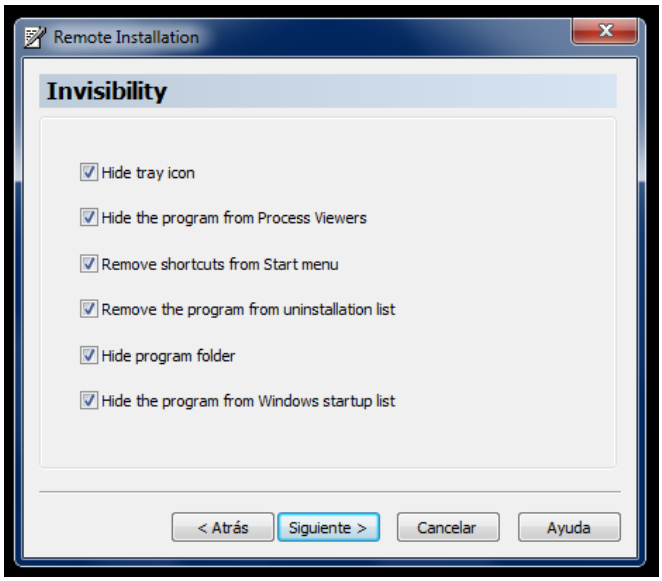


Figura 6.4. Invisibilidad del keylogger

4. En la cuarta pantalla se encuentra la seguridad del keylogger, es decir aquí se puede habilitar una contraseña para abrir los archivos o logs que serán generados por el

keylogger, en caso de habilitar la contraseña existen varias opciones de lo que va a ser protegido con la misma.

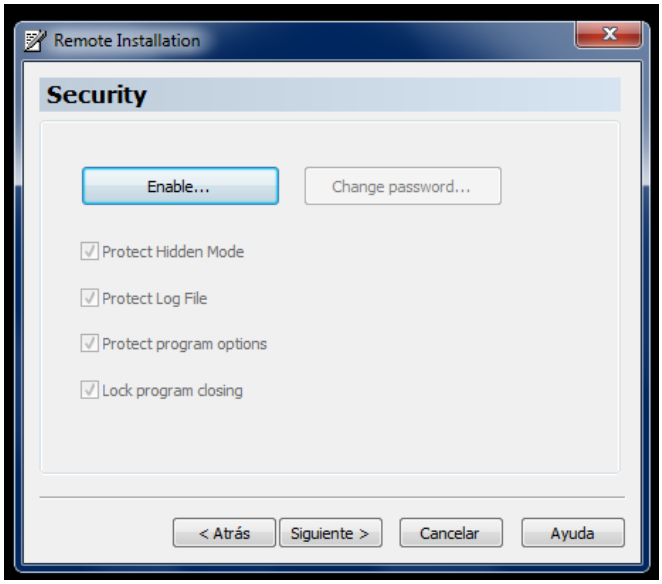


Figura 6.5. Clave de seguridad del keylogger

5. En la quinta pantalla se habilita la contraseña para los logs, archivos, vistas, etc.

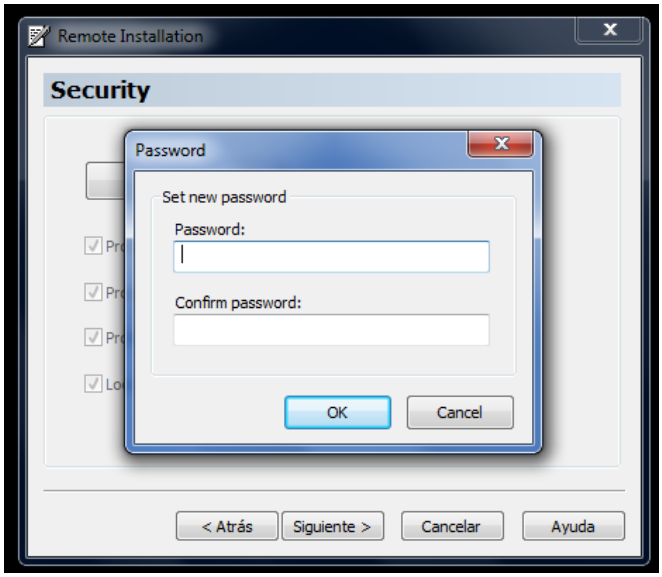


Figura 6.6. Configuración de contraseña

6. Se escribe la contraseña y se la confirma.

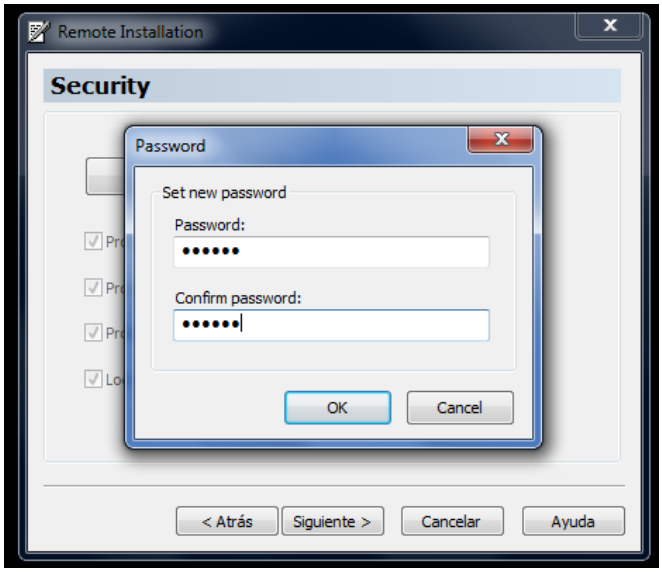


Figura 6.7. Confirmación de contraseña

7. Una vez habilitada la contraseña existe la opción de deshabilitarla o cambiarla y seleccionar qué es lo que va a proteger la nueva contraseña.

Figura 6.8. Opciones de seguridad del keylogger

8. En la pantalla de actualizaciones Web, se puede escoger: si se desea que busque actualizaciones, que se actualice automáticamente o que se actualice en ese momento; pero lo recomendable es no seleccionar ninguna de ellas, para que no sea detectado en el momento de realizar dichas actualizaciones.

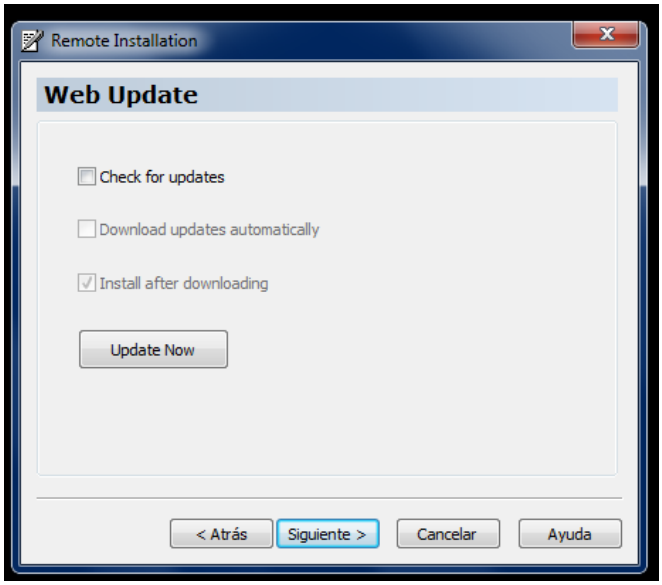


Figura 6.9. Actualizaciones de keylogger

9. En las siguientes opciones se puede seleccionar si se desea que inicie cuando se arranca Windows, que inicie en modo escondido, indica cuáles son las teclas que se deben presionar para poder ingresar al keylogger cuando inicia en modo escondido e indica la opción también de que se autodestruya y en qué fecha. Lo recomendable es que inicie cuando inicia Windows y que lo haga en modo escondido.

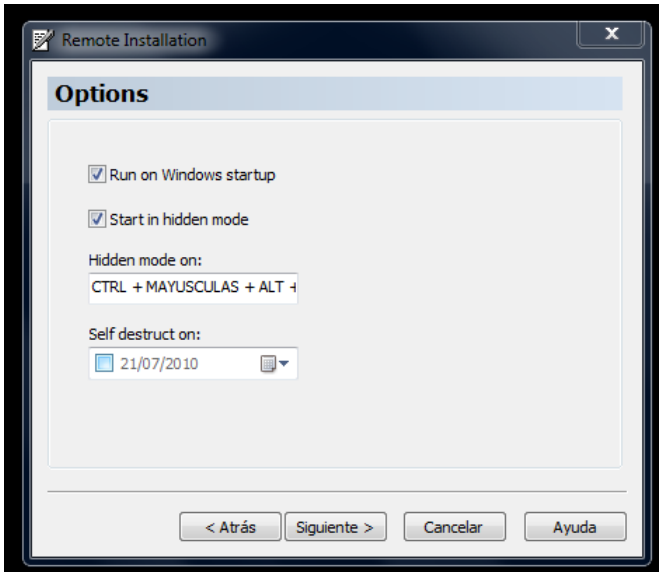


Figura 6.10. Opciones de inicio del keylogger

10. En la siguiente pantalla se debe configurar cada cuanto tiempo se desea que sean enviados los logs, el método de entrega, es decir, si se quiere que sea por correo electrónico, vía FTP, etc, o se puede combinar las formas de entrega; en este caso se entregarán en un servidor FTP. Se puede escoger lo que se desea capturar; las pulsaciones, los sitios Web visitados, los chats, las pantallas; se puede escoger el formato del log, puede ser en formato Web o encriptado, de manera que puede ser visualizado únicamente en el visor de logs de Ardamax; y por último se puede escoger el peso mínimo de los logs para que sean enviados.

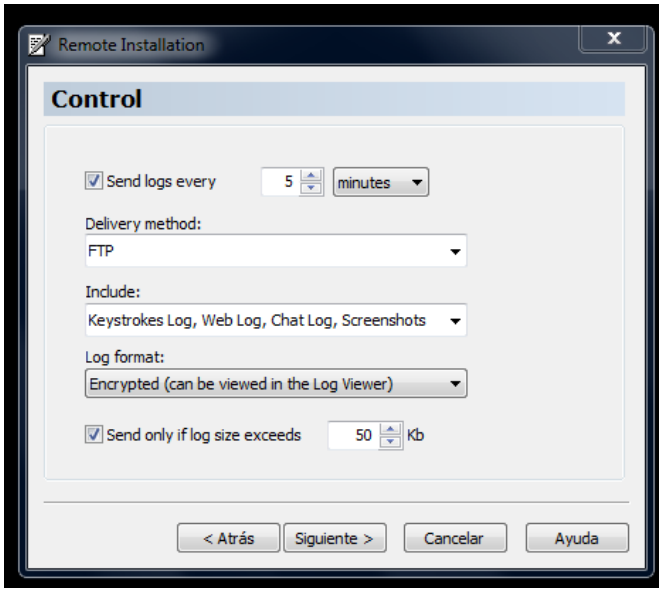


Figura 6.11. Opciones de envío de logs

11. Ahora según el caso se debe configurar donde se realizará la entrega de los logs, en este caso es configurado el servidor FTP. Para iniciar se ingresa la dirección del host a donde se enviarán los archivos; se ingresa el nombre de la carpeta donde se los guardará, el puerto mediante el cual se ingresa en el servidor y se pone el nombre y la contraseña del servidor FTP. Para comprobar que se reciban los logs existe la opción de realizar un test o prueba.

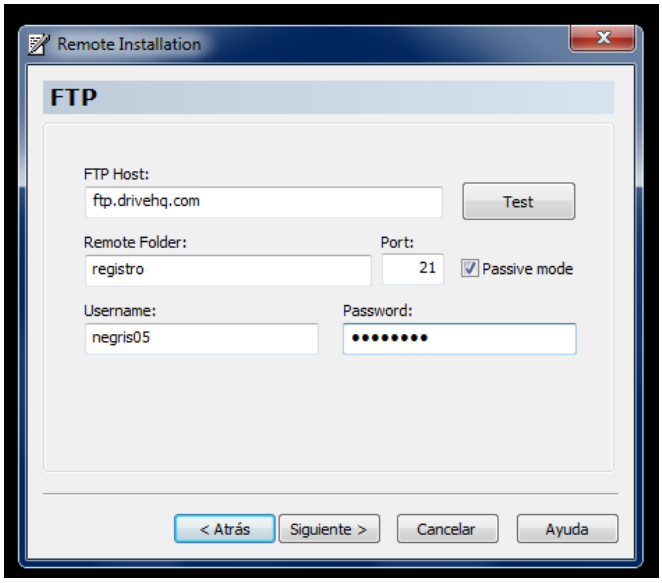


Figura 6.12. Datos del servidor FTP

12. Una vez realizado este test, el keylogger despliega una pantalla en la que indica que la entrega de prueba fue exitosa, por lo que los logs llegarán correctamente.

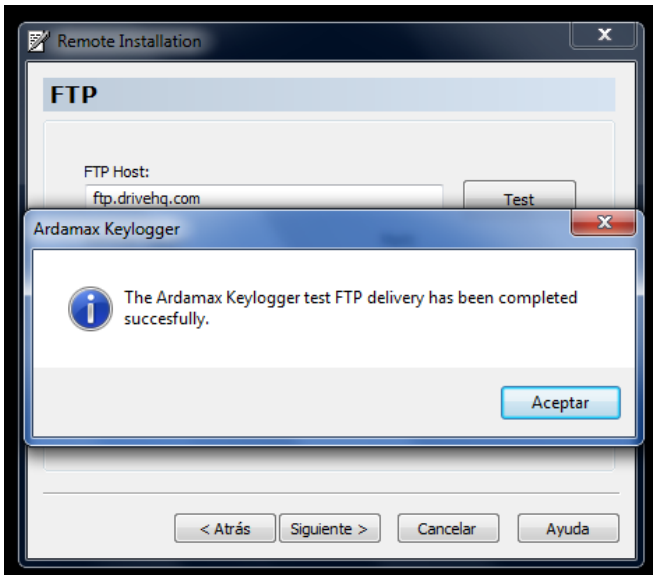


Figura 6.13. Prueba de conexión con el servidor FTP exitosa

13. Después se puede escoger que es lo que va a estar habilitado para los logs; en este caso se seleccionan todas las opciones para ver qué información podemos obtener.

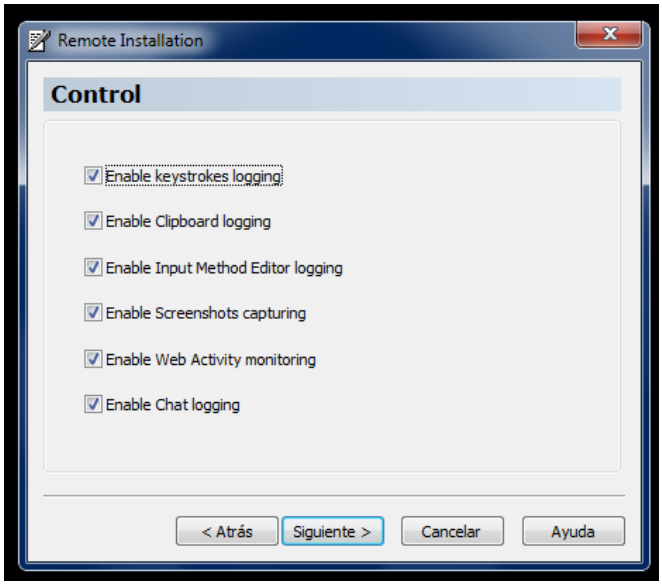


Figura 6.14. Opciones de lo que capturará el keylogger

14. Si se desea capturar pantallas, se puede definir el tiempo entre cada captura, se puede definir si se requiere la pantalla completa y la calidad de la imagen.

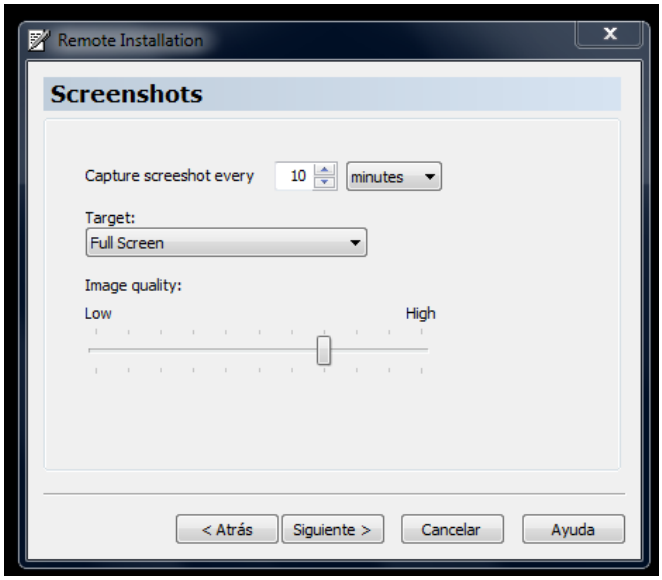


Figura 6.15. Opciones de captura de pantalla

15. Luego de configurar todas las opciones antes mencionadas, se debe indicar dónde se va a crear el archivo de instalación y para evitar sospechas en la víctima podemos cambiar el ícono con el que va a ser creado el instalador.

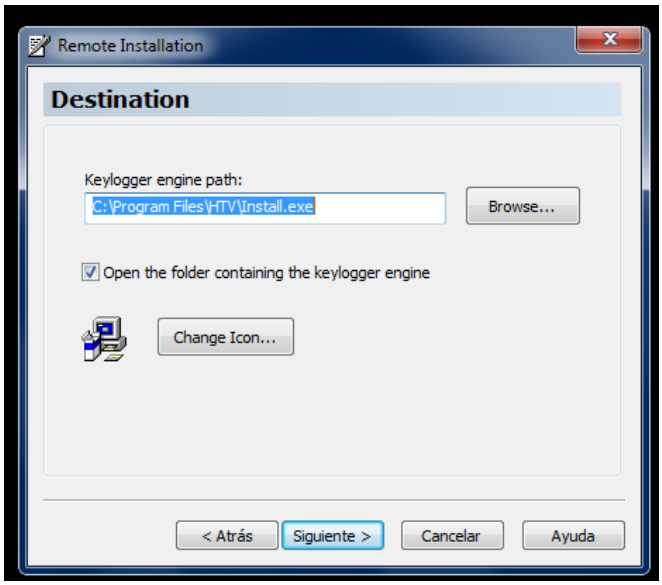


Figura 6.16. Carpeta donde se creará el instalador

16. Aparece una pantalla de resumen del keylogger, antes de indicar que el instalador fue creado.

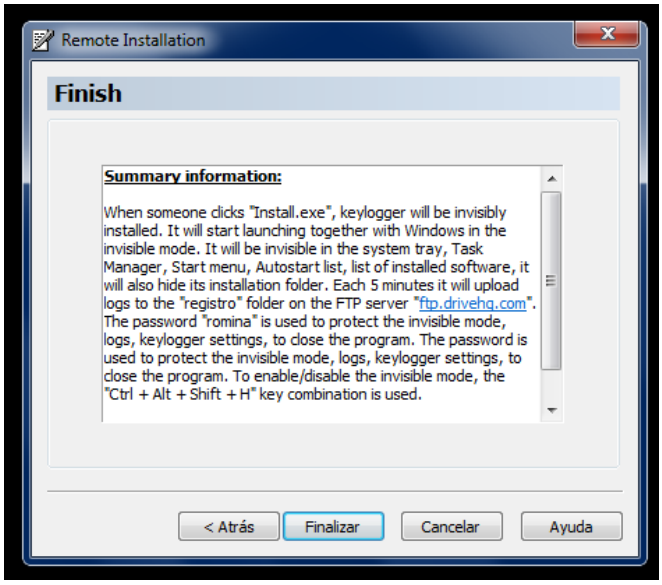


Figura 6.17. Resumen del keylogger

17. Por último despliega una pantalla con un mensaje indicando que el paquete o instalador fue creado exitosamente.

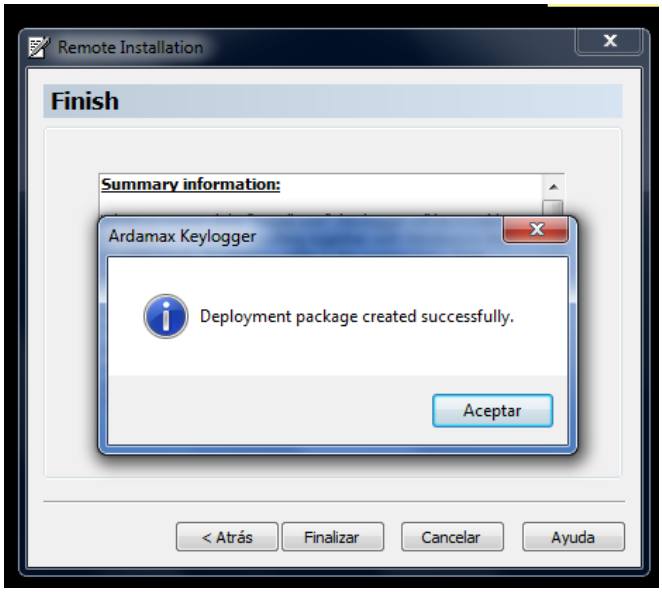


Figura 6.18. Creación del instalador satisfactoria

18. Aquí se puede observar con el ícono de una imagen el archivo Install, con el cual se generará el ataque.

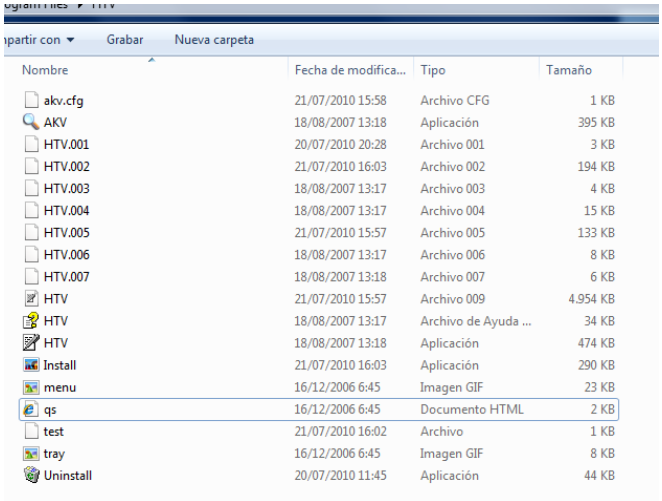


Figura 6.19. Instalador creado

Una vez creado el instalador del keylogger se lo unió a una imagen, de manera que, al momento que la víctima abrió el archivo, puede observar una imagen común y automáticamente se instaló el keylogger en un segundo plano sin levantar sospechas.

Para poder unir el keylogger a la imagen se necesita un programa que lo haga, en este caso se utilizó el programa Uticasoft SFX Compiler[20]; el procedimiento a seguir para crear un solo archivo es el siguiente:

Se abre el programa y despliega esta pantalla, en la que se abren los archivos que se desea unir.

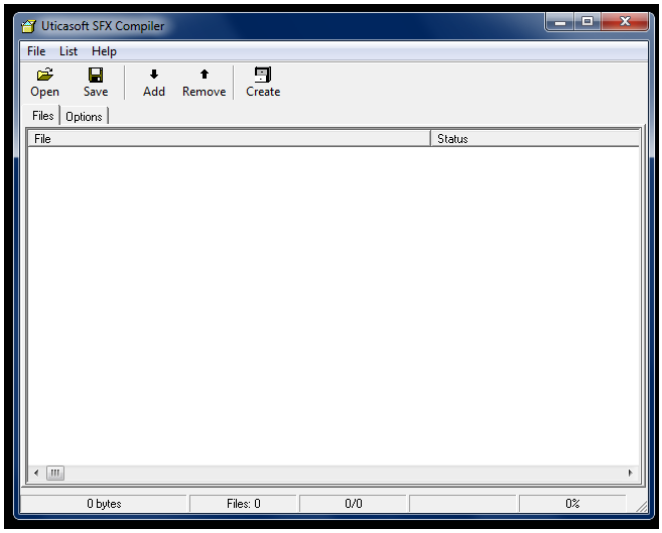


Figura 6.20. Inicio compilador de archivos

Se añaden los archivos uno por uno, para este caso el instalador.

[20] Programa con licencia gratuita, creado por Jobin Rezai.

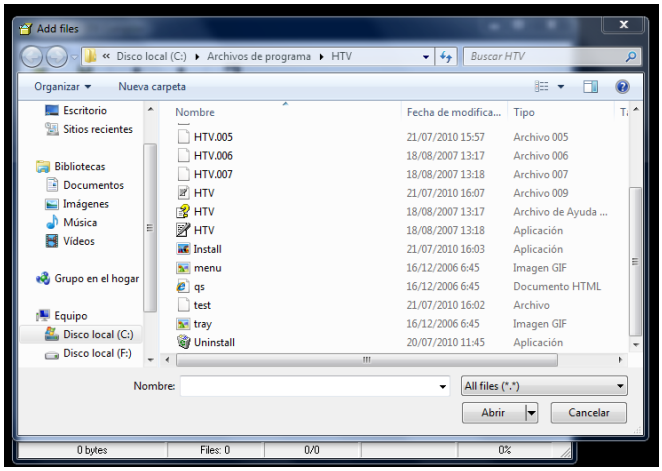


Figura 6.21. Añadir instalador de keylogger

Se añade el siguiente archivo, es decir, la imagen.

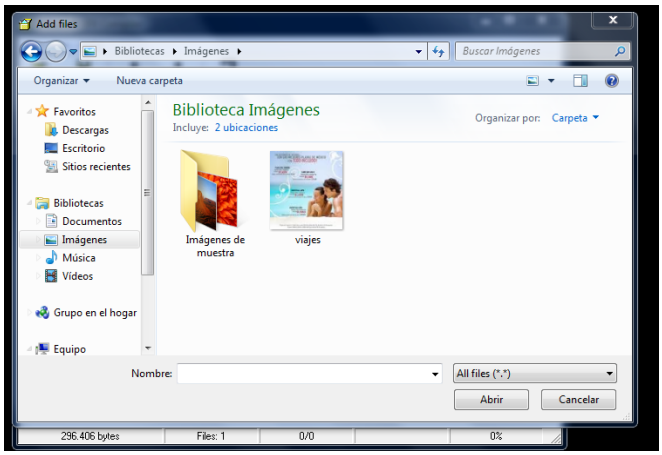


Figura 6.22. Añadir imagen

En esta pantalla se puede observar que los archivos fueron abiertos y están listos para ser unidos, pero antes, deben ser configuradas las opciones de orden de ejecución de los archivos.

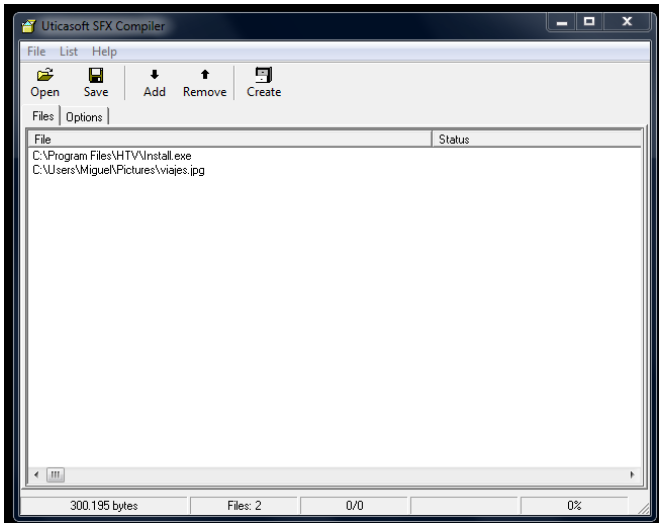


Figura 6.23. Archivos que serán compilados

En la pestaña Options se puede escoger que archivo se desea ejecutar primero y cual después de la extracción, existen más opciones pero en este caso no serán utilizadas.

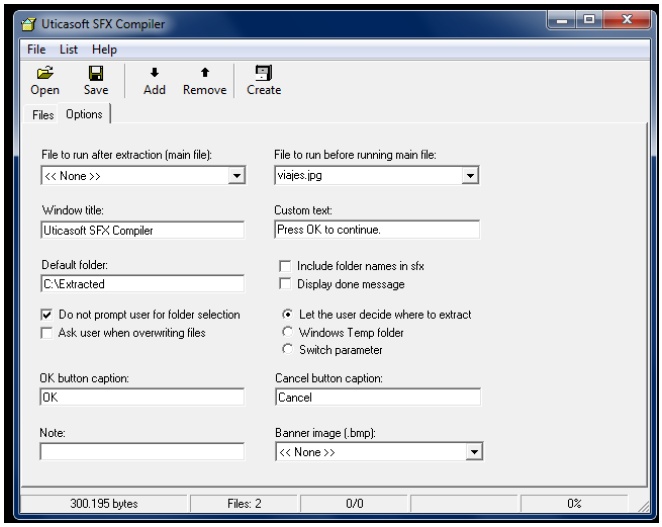


Figura 6.24. Opciones de ejecución

En base a las necesidades de este estudio, primero debe ejecutarse la imagen viajes.jpg y luego de la extracción el archivo Install.exe.

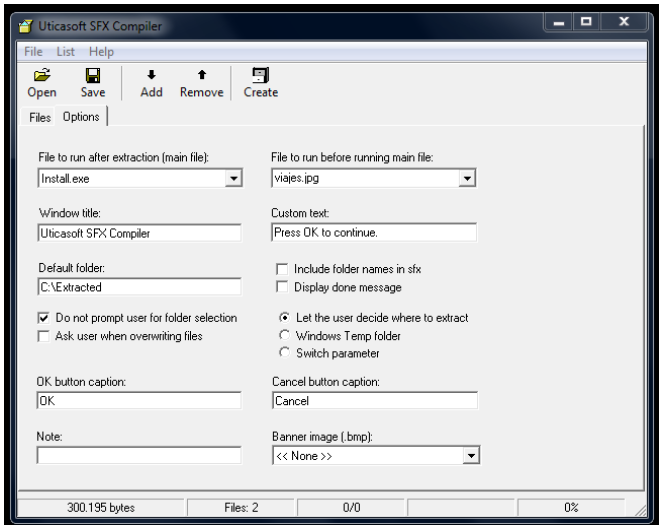


Figura 6.25. Archivo que se ejecuta primero

Se debe presionar el botón Create y escoger en donde se desea crear el archivo unido y que el nombre con el que lo vamos a identificar..

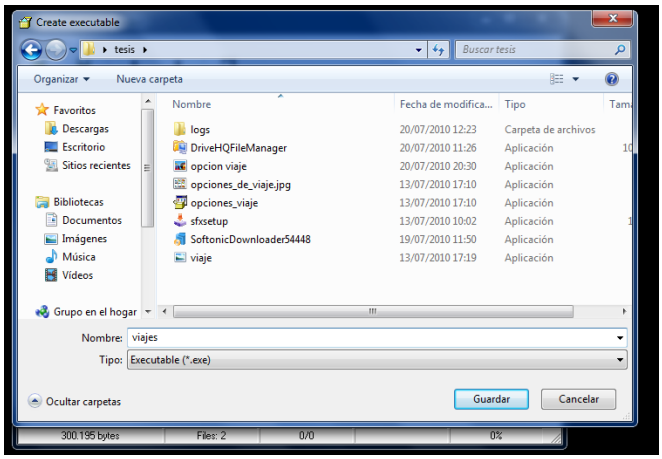


Figura 6.26. Carpeta de creación de archivo

Se lo guarda y se despliega un mensaje en el que indica que el archivo fue creado exitosamente.

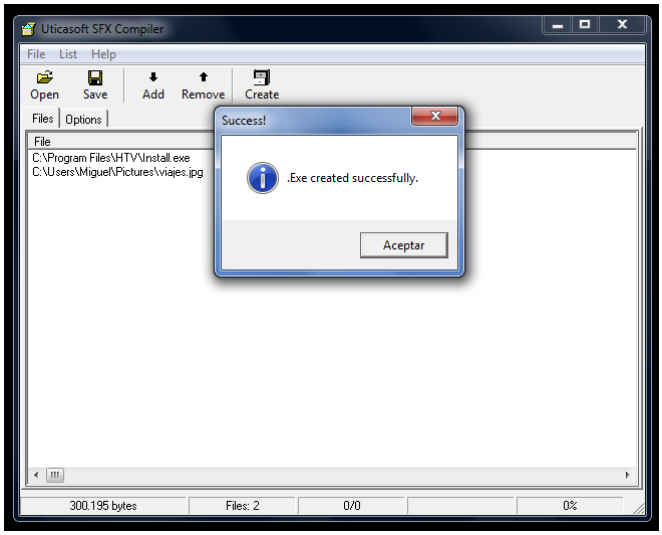


Figura 6.27. Creación exitosa

En esta lista de archivos, se puede observar el archivo viajes que fue unificado.

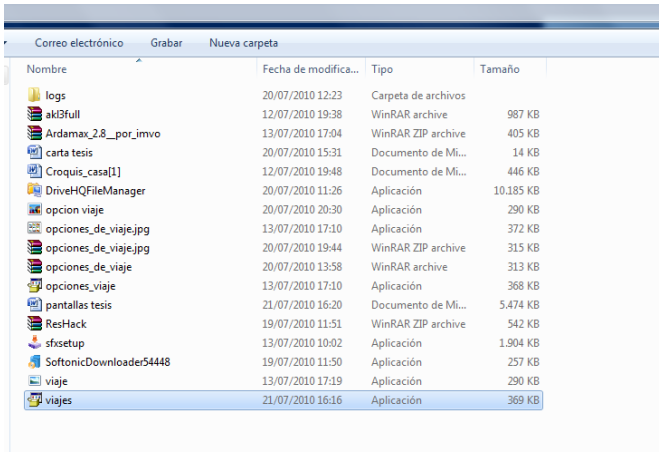


Figura 6.28. Archivo creado

Cuando ya se ha unificado el instalador y la imagen, se obtuvo un solo archivo, el mismo que tiene el ícono de un archivo ejecutable, por lo que es probable que la víctima no se sienta segura de abrirlo. Para evitar este problema existe la opción de cambiar el ícono del archivo, de manera que parezca una imagen normal y no genere dudas en la persona que la

va a abrir; para esto será utilizado otro programa; en este caso se usará el Resource Hacker[21].

El procedimiento para cambiar este ícono es el siguiente:

Se ejecuta el programa y aparece una pantalla en la que se abre el archivo del que se cambiará el ícono.

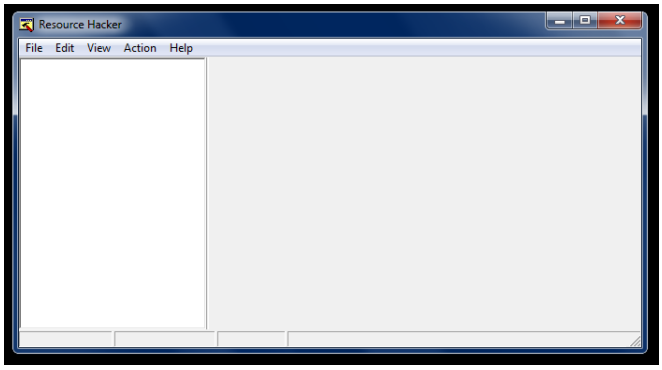


Figura 6.29. Inicio de Resource Hacker

Se abre el archivo viajes.

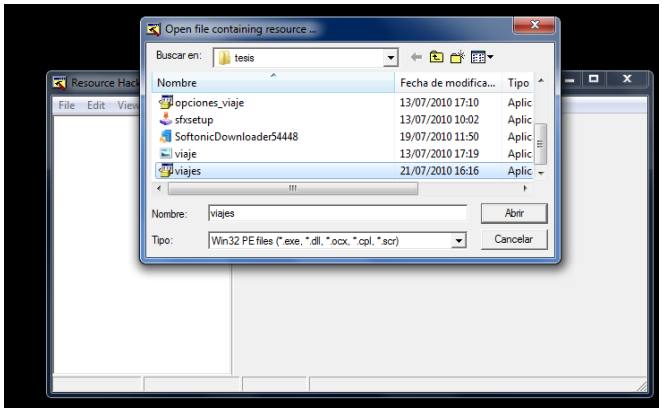


Figura 6.30. Escoger el archivo

[21] Programa con licencia gratuita, creado por Angus Johnson.

En la pantalla inicial aparecerán varias carpetas, dentro de estas existe una llamada Icon. Dentro de ésta se encuentra otra carpeta, la cual puede tener diversos nombres y dentro de la misma encontramos un archivo; si se le da click aparecerá la imagen del ícono que tiene actualmente el archivo.

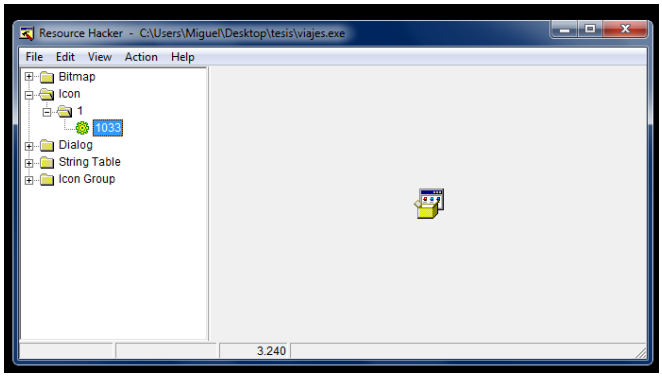


Figura 6.31. Icono que se cambiará

Se debe dar click derecho sobre ese archivo y seguidamente dar click sobre Replace Resource para cambiar la imagen del ícono.

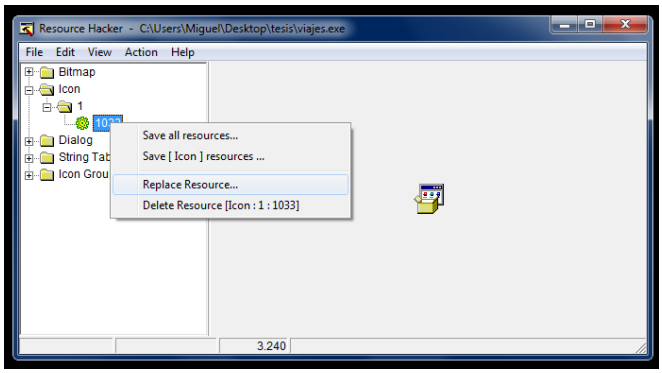


Figura 6.32. Reemplazo de figura

Aparece una pantalla en la que se debe abrir el archivo del cual se va a escoger la imagen que reemplazará la actual.

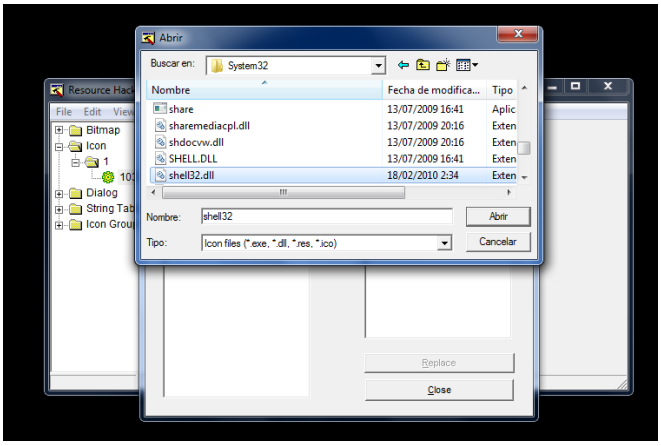


Figura 6.33. Archivo con íconos nuevos

Si se ingresa en el archivo de los íconos de Windows, se puede escoger la imagen de un video, una imagen, etc.

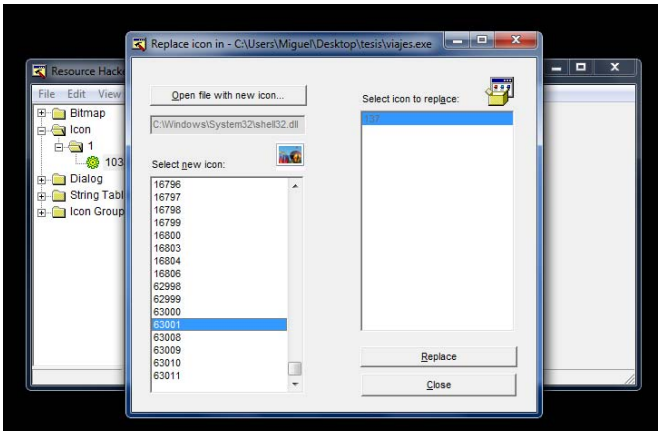


Figura 6.34. Nuevo ícono del archivo

Una vez elegida la nueva imagen, se puede observar que cambia el dibujo anterior y que aparece el que se escogió.

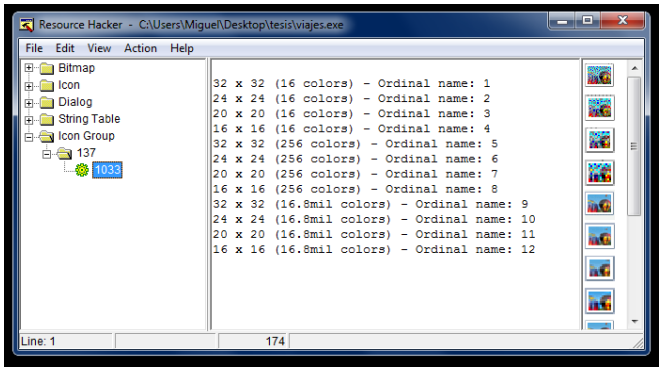


Figura 6.35. Icono reemplazado

Se despliega una pantalla en la que pregunta si se desean guardar los cambios realizados en el ícono.

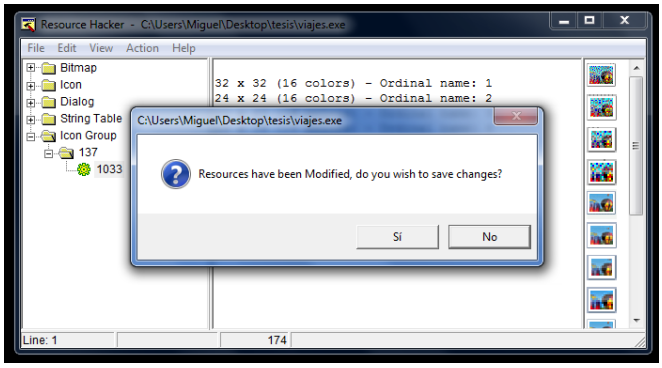


Figura 6.36. Guardar los cambios

Se indica el lugar en el que se va a guardar el archivo con el nuevo ícono.

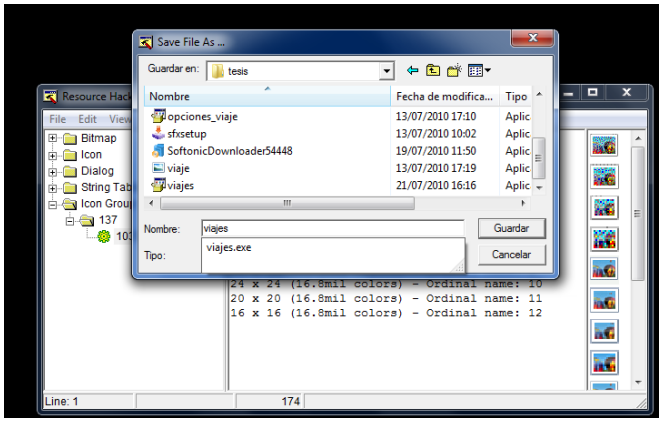


Figura 6.37. Carpeta destino

En esta pantalla observamos el archivo unificado ya con el ícono de una imagen normal.

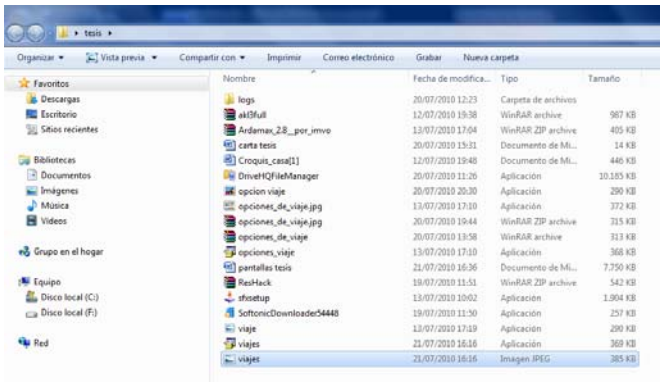


Figura 6.38. Archivo con nuevo ícono

Una vez que se realizó todo el proceso antes mencionado y se tiene el instalador listo para que el usuario o víctima lo abra, se debe encontrar un método para que este archivo llegue a manos de la persona en cuestión sin sospechar de que se trata; en este caso la víctima es la Jefe de Ventas de una empresa que importa y distribuye medios de cultivo para laboratorios clínicos, industriales y farmacéuticos.

La persona que lleva a cabo el ataque, tiene relación con la víctima; motivo por el cual, sabe que la víctima es cliente de un almacén grande del país, el mismo que constantemente realiza sorteos con sus clientes. Al tener esta información, se grabó el archivo con el instalador del keylogger en un cd y se redactó una carta; en la que se indicaba que la víctima era la ganadora de un sorteo en dicho almacén y el premio era un viaje y se le pedía que abra el archivo del cd para que escogiera el destino al cual deseaba viajar.

Es habitual que, estas promociones o premios atraigan mucho a la gente, que en el país todavía es muy ingenua y no toma las precauciones adecuadas antes de dejarse llevar por este tipo de engaños; de manera que, efectivamente esta persona abrió el archivo y se instaló el keylogger en su máquina.

Una vez instalado el programa, se pudo obtener información, que en caso de ser de la competencia sería muy útil.

Para poder usar los logs generados por el keylogger, se debe seguir el siguiente procedimiento:

En el servidor FTP se guardan los logs, los mismos que pueden descargar uno por uno o mediante la instalador de una administrador de archivos del mismo sitio, se pueden descargar todos o los que se deseen.

En la siguiente imagen, se puede observar que el administrador de archivos está conectado y que se debe indicar en que carpeta se desea guardar los archivos que se descargarán del servidor.

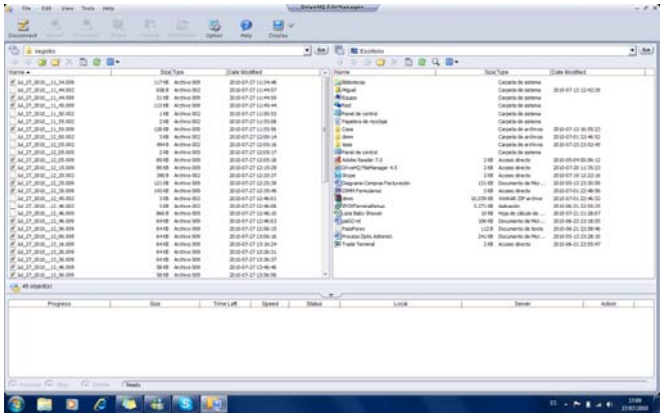


Figura 6.39. Administrador de archivos FTP

Una vez escogida la carpeta en la que se guardarán los archivos, se seleccionan los archivos que se van a descargar y se presiona el botón de descarga o download.

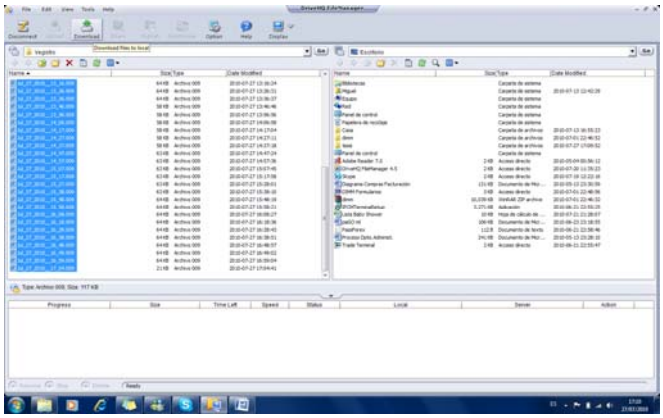


Figura 6.40. Descarga de archivos

Cuando se han descargado los archivos, se observa que efectivamente los logs se encuentran en el lugar que fue seleccionado.

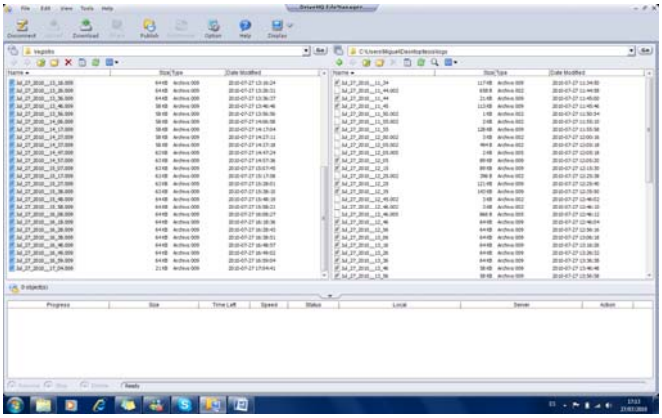


Figura 6.41. Archivos descargados

Si se abre la carpeta en la que se guardaron estos registros, se puede constatar que ahí están los archivos descargados.

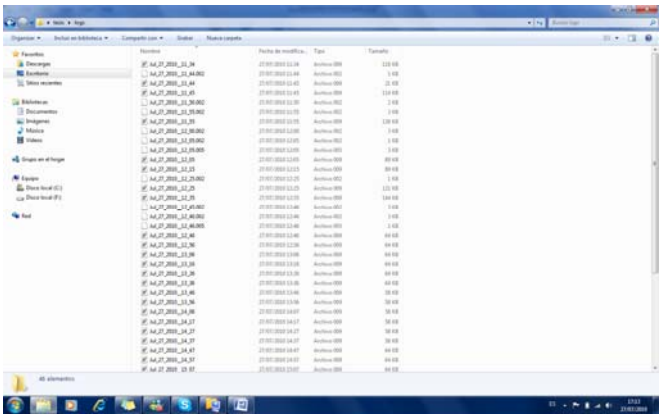


Figura 6.42. Logs del keylogger

Para poder visualizar estos archivos, se debe abrir el visualizador de logs o keylogger viewer; una vez abierto, se deben abrir los archivos descargados, por lo que ingresamos en la ubicación en la que se guardaron los logs y se los abre.

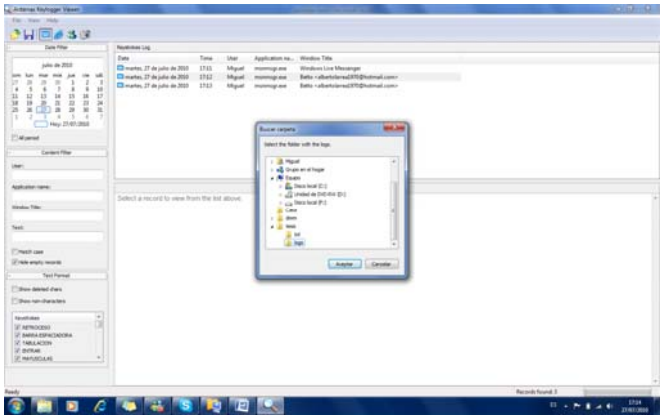


Figura 6.43. Abrir logs en visor de logs

Cuando se abrieron estos archivos, se observa una lista en la que constan los archivos con la fecha de creación, la hora, el usuario del que se generaron los logs, la aplicación de la que se tomaron las capturas y el título de la ventana en la que se estaba trabajando.

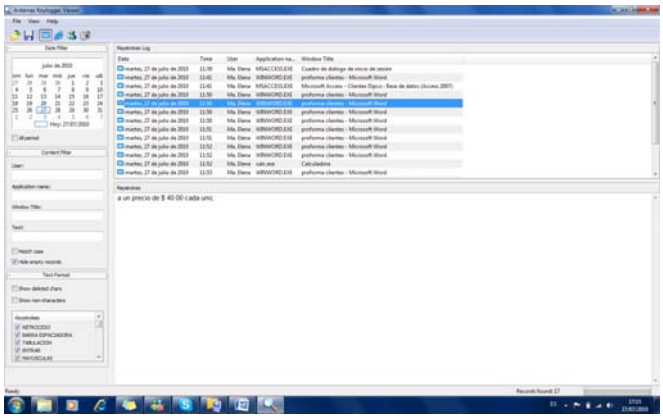


Figura 6.44. Lista de logs

A continuación, se puede observar que si se da un click en cualquiera de los archivos, en la parte inferior de la lista aparecen los datos que fueron capturados en ese archivo.

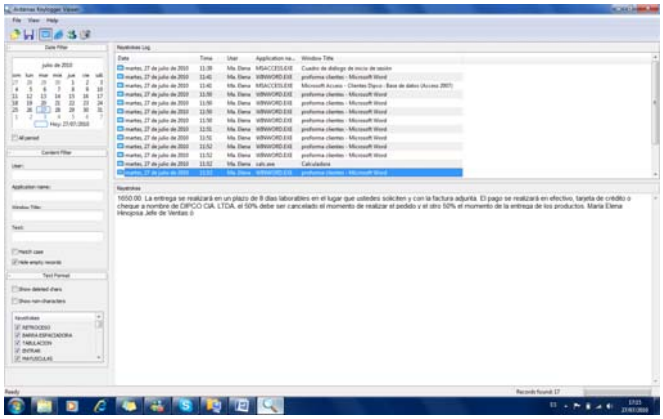


Figura 6.45. Contenido de un log

En este caso por ejemplo, observamos que se capturó el usuario y la contraseña de un correo electrónico gratuito.

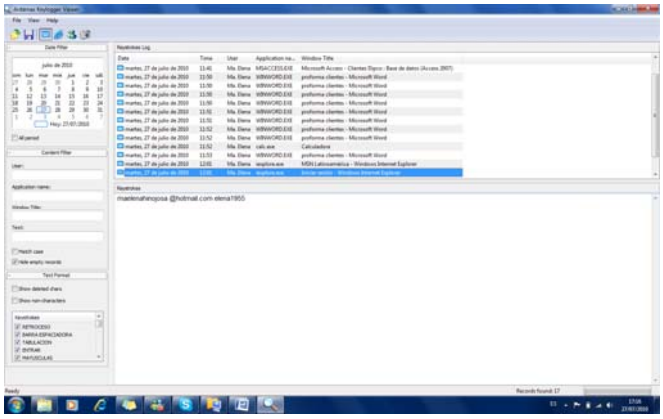


Figura 6.46. Datos capturados

En las pantallas anteriores, se puede observar que existen valores, nombres de productos, etc.

De esta manera se puede demostrar que se puede obtener información muy valiosa a través de un ataque de ingeniería social, que todas las herramientas necesarias están al alcance de nuestras manos, son gratuitas y simplemente se necesita estudiarlas y aprender como funcionan para sacarles el mayor provecho posible.

En el anexo # se pueden encontrar varios de los archivos con información capturada con este ejerció práctico, por efectos de seguridad los nombres y datos confidenciales han sido cambiados.

6.2. ESTUDIO DIAGNOSTICO DEL CONOCIMIENTO EMPRESARIAL SOBRE INGENIERIA SOCIAL

Para realizar un estudio diagnóstico sobre el conocimiento que se tiene sobre la ingeniería social en nuestro medio, se realizaron tres tipos de encuestas en una empresa de nuestra ciudad, se realizó una primera encuesta a los usuarios finales de los sistemas (empleados, secretarias, asistentes, etc), una segunda encuesta a varios jefes departamentales y de unidad y una tercera encuesta a los administradores de los sistemas y aplicaciones.

6.2.1 Análisis e interpretación

6.2.1.1 Encuestas a Administradores de Sistema

1.- Conoce usted lo que es la Ingeniería Social?

El 30% de personas coinciden en que si conocen la ingeniería social; y la mayoría opina que es una técnica que se utiliza para obtener información confidencial y obtener algún beneficio, el 70% señala que no conoce lo que es la ingeniería social.

2.- Revisa los antecedentes de las personas que van a trabajar con usted?

El 100 % de personas que respondieron la encuesta indican que si revisan los antecedentes de las personas que van a trabajar con ellos, que van a tener acceso a los sistemas, a la información, etc.

3.-La gente de seguridad de su empresa tiene acceso a información de la infraestructura de la misma?

El 20% de personas indican que el personal de seguridad de la empresa si tiene acceso a información de la infraestructura de la misma, el 80% dice que el personal de seguridad no tiene acceso a esta información.

4.- Es pro-activo en cuanto a la capacitación de su personal

El 70% de personas coinciden en que si son proactivos en lo que se refiere a la capacitación del personal que tiene a su cargo, el 30% señala que no es proactivo en cuanto a capacitación se refiere.

5.- De qué manera desecha un correo electrónico impreso con información confidencial

El 30% de personas indica que rompe los correos electrónicos, el 40% de personas coincide en que bota los correos electrónicos y el 30% señala que tritura los correos electrónicos que contienen información confidencial.

6.- Ha detectado usted ataques de ingeniería social dentro de su empresa

El 70% de personas que contestaron la encuesta señala que no ha detectado ataques de ingeniería social dentro de la empresa, mientras que el 30% indica que si han detectado ataques de ingeniería social dentro de su empresa.

7.- Los ataques detectados dentro de la empresa fueron

El 67% de personas señala que los ataques de ingeniería social detectados fueron internos, y el 33% indica que los ataques detectados fueron externos.

8.- Se realizaron acciones de seguridad para evitar ser víctimas de un nuevo ataque de ingeniería social

El 100 % de personas que respondieron la encuesta indican que se tomaron medidas de seguridad contra los ataques de ingeniería social detectados dentro de la empresa.

9.- Fue denunciado el ataque de ingeniería social? Porqué

El 100 % de personas señalan que no se denunciaron los ataques detectados, debido a que si los ataques eran denunciados la empresa iba a perder credibilidad.

6.2.1.2 Encuestas a Jefes Departamentales

1.- Conoce usted lo que es la Ingeniería Social?

El 80% de personas coinciden en que si conocen la ingeniería social; y la mayoría opina que es una técnica para conseguir información confidencial para obtener una ganancia o perjudicar a alguien, el 20% señala que no conoce lo que es la ingeniería social.

2.- Conoce cómo se lleva a cabo un ataque de ingeniería social?

El 70% de personas que respondieron la encuesta indican que si saben como se lleva a cabo un ataque de ingeniería social, mientras el 30% señala que no conoce como se realiza un ataque de este tipo.

3.- Considera usted, que es fácil obtener información confidencial del personal de una compañía mediante una llamada telefónica, sin necesidad de identificarse?

El 100 % de personas indican que es fácil obtener información confidencial del personal de una empresa a través de una llamada telefónica sin necesidad de identificarse.

4.- De qué manera desecha un correo electrónico impreso con información confidencial?

El 60% de personas indica que rompe los correos electrónicos, el 10% de personas coincide en que bota los correos electrónicos y el 30% señala que tritura los correos electrónicos que contienen información confidencial.

5.- Ha detectado usted ataques de ingeniería social dentro de su empresa?

El 60% de personas que contestaron la encuesta señala que no ha detectado ataques de ingeniería social dentro de la empresa, mientras que el 40% indica que si han detectado ataques de ingeniería social dentro de su empresa.

6.- Los ataques detectados dentro de la empresa fueron internos o externos?

El 50% de personas señala que los ataques de ingeniería social detectados fueron internos, y el 50% indica que los ataques detectados fueron externos.

7.- Se realizaron acciones de seguridad para evitar ser víctimas de un nuevo ataque de ingeniería social?

El 100 % de personas que respondieron la encuesta indican que se tomaron medidas de seguridad contra los ataques de ingeniería social detectados dentro de la empresa.

8.- Fue denunciado el ataque de ingeniería social? Porqué?

El 75% de personas señalan que no se denunciaron los ataques detectados, debido a que si los ataques eran denunciados la empresa iba a perder credibilidad, el 25% indica que si se denunciaron los ataques detectados.

6.2.1.3 Encuestas a Usuarios Finales

1.- Conoce usted lo que es la Ingeniería Social?

El 43% de personas coinciden en que si conocen lo que es la ingeniería social, mientras el 57 % señala que no conoce lo que es la ingeniería social.

2.- Puede determinar si ha sido víctima de un ataque de ingeniería social?

El 84% de personas que respondieron la encuesta indican que no podrían determinar si han sido víctimas de algún tipo de ataque de ingeniería social, y el 16% señala que si podría determinar si ha sido víctima de un ataque.

3.- Cree usted que una llamada telefónica de un jefe o del personal de soporte puede ser un ataque de ingeniería social?

El 68% de personas indican que no creen que una llamada telefónica de un jefe o de personal que da soporte en la empresa sea un ingeniero social llevando a cabo un ataque, sin embargo, el 32% señala que una llamada de estas personas podría tratarse de un ataque de ingeniería social.

4.- Corrobora usted la identidad de quien realiza una llamada telefónica?

El 63% de personas indica que si corrobora la identidad de las personas que le llaman, y el 37% señala que no corrobora la identidad de las personas que se encuentran del otro lado del teléfono.

5.- De qué manera desecha un correo electrónico impreso con información confidencial?

El 74% de personas indica que rompe los correos electrónicos, el 21% de personas coincide en que bota los correos electrónicos y el 5% señala que tritura los correos electrónicos que contienen información confidencial.

6.- Tiene usted y su compañía políticas de cambio periódico de contraseña

El 95% de personas que contestaron la encuesta señala que la compañía si cuenta con un cambio periódico de contraseñas en los sistemas y las máquinas, mientras el 5% indica que no existe una política de cambio de contraseñas en la empresa.

7.- Cuál es el tiempo máximo que debe transcurrir antes de que se le solicite el cambio de su contraseña?

El 90% de personas señalan que el cambio periódico de contraseñas en un tiempo menor a 3 meses, el 5% indica que debe cambiar su contraseña en un tiempo que varía entre 3 y 6 meses, el 5% dice que debe realizar el cambio en un lapso de 6 meses a 1 año y nadie indica que nunca cambia de contraseña.

8.- Está usted consiente del impacto que tiene que usted no corrobore cierta información?

El 63% de personas indican que si tienen conciencia sobre el impacto que tiene que no se corrobore cierta información, y el 37% señala que no sabe cual es el impacto de que no corrobore información.

9.- Cada cuanto tiempo la empresa realiza capacitaciones para mejorar el nivel de conocimiento del personal?

Nadie señalan que la empresa realiza capacitaciones en un tiempo menor a 3 meses, el 10% indica que asiste o conoce de capacitaciones en un tiempo que varía entre 3 y 6 meses, el 37% dice que debe se realizan capacitaciones en un lapso de 6 meses a 1 año y el 53% indica que nunca hay capacitaciones para el personal de la empresa.

10.- Bloquea usted su terminal cuando sale de su puesto de trabajo?

El 89% de personas indican que si bloquea su terminal cuando sale de su puesto de trabajo, y el 11% señala que no bloquea su terminal cuando se retira de su puesto de trabajo

11.- Tiene su nombre y/o password anotado en algún lugar visible?

El 100 % de personas que respondieron esta encuesta indican que no tienen su nombre o usuario y password en un lugar visible.

12.- Se asegura usted de la autenticidad de los remitentes de los correos electrónicos que recibe?

El 68% de personas señalan que no se percata de quien es el remitente de los correos electrónicos que recibe, y el 32% indicó que si se asegura de quien es el remitente de dichos correos.

13.- Se asegura usted de que una empresa de servicios es la autora de un correo electrónico de confirmación de datos?

El 89% de personas señalan que no se aseguran de que una empresa de servicios sea la autora de un correo electrónico, mientras el 11% indicó que si se asegura de cuál es la empresa que remitió el correo.

14.- Accede usted a cualquier link que le envían en los correos electrónicos?

El 89% de peronas que respondieron a esta encuesta indican que no acceden a cualquier link que tengan en un correo electrónico, si embargo, el 11% aseguró que si accede a cualquier link que le envien en un correo electrónico.

15.- Verifica usted el remitente cuando va a abrir algún archivo adjunto a un correo electrónico?

El 73% de personas señalan que si verifican quien es el remitente del correo antes de abrir un archivo adjunto, y el 47% dijeron que no verifican quien es el remitente del correo electrónico antes de abrir un archivo adjunto.

16.- Incluye usted información sensible en sus tarjetas de presentación?

El 89% de personas indican que no incluyen información sensible en sus tarjetas de presentación, mientras el 11% afirmaron que si incluyen en las tarjetas de presentación.

6.2.2 Generalización

Una vez realizadas encuestas, la tabulación de las mismas y el análisis e interpretación de cada una de ellas, podemos sacar conclusiones y dar recomendaciones a cada una de estas conclusiones en base a los resultados obtenidos de dichas encuestas. A continuación se emitirá una conclusión con la recomendación respectiva para cada pregunta de cada uno de los tres tipos de encuestas realizados:

Encuestas realizadas a Administradores de Sistemas:

1.-

Conclusión.- Al dimensionar las respuestas de la consulta referente al conocimiento de qué es la Ingeniería Social podemos concluir, que en las empresas de nuestro país no existe una conciencia real acerca de la seguridad de la información, puesto que como podemos observar en la gráfica inclusive el personal dedicado a la administración de los sistemas de información no tiene una percepción clara de este concepto, teniendo en cuenta que para muchas empresas la información es uno de los activos más importantes en el desarrollo de sus operaciones.

Recomendación.- Planificar estrategias de seguridad de la información que inicien con la concienciación al personal de las empresas acerca de la importancia que representa la información, los controles y procedimientos que rigen la seguridad de la misma.

2.-

Conclusión.- Una vez obtenidos los resultados sobre si se revisan los antecedentes de las personas que van a formar parte del equipo de trabajo podemos concluir, que en las empresas de nuestro país si se revisan los antecedentes de las personas que van a trabajar ahí; de manera que de cierto modo si se tiene un control sobre las personas que van a tener acceso a información confidencial y que puede poner en riesgo a la empresa o a las personas que forman parte de ella.

Recomendación.- Mantener este control sobre los antecedentes de las personas que ingresan a la empresa y van a formar parte del equipo de trabajo, teniendo en cuenta el tipo de información a la que van a tener acceso.

3.-

Conclusión.- Después de calcular las respuestas sobre si el personal de seguridad tiene acceso a información de infraestructura de la empresa podemos concluir, que en nuestro país las empresas no tienen una conciencia real del impacto que puede traer que este tipo de personal tenga acceso a cierta información, ya que aparentemente la gente de seguridad no podría usar estos datos, pero en realidad podrían sacar un gran provecho de tener esta información en sus datos y traer problemas de gran magnitud para la empresa como tal o para las personas que se encuentran trabajando ahí.

Recomendación.- Conservar toda la información sobre la infraestructura de la empresa bajo un estricto control, para que solo el personal autorizado pueda accesar a la misma y no cualquier persona.

4.-

Conclusión.- Luego de dimensionar los resultados sobre si se tiene una pro-actividad en cuanto a la capacitación del personal se trata podemos concluir, que en las empresas de nuestro país no se tiene un conocimiento real sobre lo importante que es mantener una capacitación constante del personal sobre la seguridad de la información y sobre la importancia que tiene cierto tipo de información para la empresa y las pérdidas que puede ocasionar un mal manejo de la misma.

Recomendación.- Elaborar un plan de capacitación para todo el personal sobre la importancia de la información y sobre la seguridad de la misma, los riesgos que se presentan y las maneras adecuadas de resguardarla.

5.-

Conclusión.- Cuando se han obtenido las respuestas sobre la manera en la que son desechados los correos electrónicos con información confidencial podemos concluir, que en nuestras empresas no se tiene una conciencia adecuada sobre el valor que puede tener

para un hacker cualquier tipo de información, peor aún si hablamos de información confidencial; la gráfica nos muestra que muy pocas personas trituran esta información, que es la manera adecuada de desechar esto.

Recomendación.- Crear una campaña sobre la manera adecuada de desechar documentos que contengan información valiosa, ya sea para la empresa o para una persona en particular y brindar los medios adecuados para poder realizar esto de la manera apropiada.

6.-

Conclusión.- Una vez que se han calculado las respuestas sobre la detección de ataques de ingeniería social dentro de la empresa podemos concluir, que en las empresas del Ecuador no se han detectado gran cantidad de ataques de ingeniería social, en su mayoría debido al desconocimiento que hay sobre como se llevan a cabo; sin embrago existe un porcentaje medio de personas que si han detectado este tipo de ataques.

Recomendación.- Concientizar a las personas sobre lo que es la ingeniería social, como se lleva a cabo un ataque de este tipo y las consecuencias que puede tener el mismo para poder identificar un ataque en su primer fase y tomar las medidas correspondientes para evitar que trascienda.

7.-

Conclusión.- Después de dimensionar las respuestas sobre el tipo de ataques que se encontraron en las empresas, ya sean internos o externos, podemos concluir, que la mayoría de ataques detectados dentro de una empresa son internos, ya que los empleados que se encuentran dentro de una organización tienen mayor acceso a información confidencial; también existen ciertos casos en los que los ataques se producen desde afuera de la empresa.

Recomendación.- Establecer una clasificación de la información, y mantener una estricto control sobre las personas que tienen acceso a la misma, especialmente si es información confidencial o top secret.

8.-

Conclusión.- Cuando se ha elaborado el resultado sobre si se tomaron acciones de seguridad sobre los ataques de ingeniería social encontrados dentro de la empresa podemos concluir, que en todos los casos se tomaron medidas de seguridad al respecto.

Recomendación.- Mantener estas acciones de seguridad y crear una bitácora con los casos presentados y la manera en la que fueron resueltos, de manera que si se presentaran nuevamente ya se sabe como se llevaron a cabo y que acciones de seguridad se tomaron.

9.-

Conclusión.- Al dimensionar las respuestas sobre si se denunciaron o no los ataques encontrados en la empresa podemos concluir, que en las empresas de nuestro país, como podemos observar en la gráfica, en ningún caso se realizó una denuncia, en su mayoría por miedo al desprestigio de la empresa.

Recomendación.- Denunciar los ataques de ingeniería social encontrados dentro de la empresa, para poder sentar un precedente y generar jurisdicción al respecto, ya que en nuestro país es muy básica la justicia en estos temas y no existe jurisdicción sobre estos temas.

Encuestas realizadas a Jefes Departamentales:

1.-

Conclusión.- Al dimensionar las respuestas de la consulta referente al conocimiento de qué es la Ingeniería Social podemos concluir, que en las empresas de nuestro país no existe una conciencia real acerca de la seguridad de la información, puesto que como podemos observar en la gráfica inclusive los Jefes departamentales no tienen una percepción clara de este concepto, teniendo en cuenta que para muchas empresas la información es uno de los activos más importantes en el desarrollo de sus operaciones.

Recomendación.- Planificar estrategias de seguridad de la información que inicien con la concienciación al personal de las empresas acerca de la importancia que representa la información, los controles y procedimientos que rigen la seguridad de la misma.

2.-

Conclusión.- Una vez obtenidas las respuestas sobre que conocimiento se tiene sobre la manera en la que se lleva a cabo un ataque de ingeniería social podemos concluir, que en las empresas ecuatorianas no se tiene un claro conocimiento sobre el proceso mediante el cual se realiza un ataque de ingeniería social, recalcando que la información es uno de los activos más valiosos con los cuenta una empresa.

Recomendación.- Enseñar al personal de las empresas cual es el proceso que sigue un ataque de ingeniería social, sus métodos y las maneras mediante las que un atacante puede obtener información general o confidencial de una persona específica o la empresa en sí.

3.-

Conclusión.- Después de valorar las respuestas sobre la facilidad que existe para obtener información mediante una llamada telefónica dentro de una empresa podemos concluir, que todas las personas que respondieron las encuestas dijeron que es muy fácil conseguir información a través de una llamada telefónica, en la mayoría de casos sin identificarse.

Recomendación.- Concientizar al personal sobre el valor que tiene la información y las medidas de seguridad y precauciones que debe tener antes de entregar cualquier tipo de información ya sea personalmente, mediante internet o vía telefónica.

4.-

Conclusión.- Cuando se han obtenido las respuestas sobre la manera en la que son desechados los correos electrónicos con información confidencial podemos concluir, que en nuestras empresas no se tiene una conciencia adecuada sobre el valor que puede tener para un hacker cualquier tipo de información, peor aún si hablamos de información confidencial; la gráfica nos muestra que muy pocas personas trituran esta información, que es la manera adecuada de desechar esto.

Recomendación.- Crear una campaña sobre la manera adecuada de desechar documentos que contengan información valiosa, ya sea para la empresa o para una persona en particular y brindar los medios adecuados para poder realizar esto de la manera apropiada.

5.-

Conclusión.- Una vez que se han calculado las respuestas sobre la detección de ataques de ingeniería social dentro de la empresa podemos concluir, que en las empresas del Ecuador no se han detectado gran cantidad de ataques de ingeniería social, en su mayoría debido al desconocimiento que hay sobre como se llevan a cabo; sin embrago existe un porcentaje medio de personas que si han detectado este tipo de ataques.

Recomendación.- Concientizar a las personas sobre lo que es la ingeniería social, como se lleva a cabo un ataque de este tipo y las consecuencias que puede tener el mismo para poder identificar un ataque en su primer fase y tomar las medidas correspondientes para evitar que trascienda.

6.-

Conclusión.- Después de dimensionar las respuestas sobre el tipo de ataques que se encontraron en las empresas, ya sean internos o externos, podemos concluir, que la mayoría de ataques detectados dentro de una empresa son internos, ya que los empleados que se encuentran dentro de una organización tienen mayor acceso a información confidencial; también existen ciertos casos en los que los ataques se producen desde afuera de la empresa.

Recomendación.- Establecer una clasificación de la información, y mantener una estricto control sobre las personas que tienen acceso a la misma, especialmente si es información confidencial o top secret.

7.-

Conclusión.- Cuando se ha elaborado el resultado sobre si se tomaron acciones de seguridad sobre los ataques de ingeniería social encontrados dentro de la empresa podemos concluir, que en todos los casos se tomaron medidas de seguridad al respecto.

Recomendación.- Mantener estas acciones de seguridad y crear una bitácora con los casos presentados y la manera en la que fueron resueltos, de manera que si se presentaran nuevamente ya se sabe como se llevaron a cabo y que acciones de seguridad se tomaron.

8.-

Conclusión.- Al dimensionar las respuestas sobre si se denunciaron o no los ataques encontrados en la empresa podemos concluir, que en las empresas de nuestro país, como podemos observar en la gráfica, en ningún caso se realizó una denuncia, en su mayoría por miedo al desprestigio de la empresa.

Recomendación.- Denunciar los ataques de ingeniería social encontrados dentro de la empresa, para poder sentar un precedente y generar jurisdicción al respecto, ya que en nuestro país es muy básica la justicia en estos temas y no existe jurisdicción sobre estos temas.

Encuestas realizadas a usuarios finales:

1.-

Conclusión.- Al dimensionar las respuestas de la consulta referente al conocimiento de qué es la Ingeniería Social podemos concluir, que en las empresas de nuestro país no existe una conciencia real acerca de la seguridad de la información, puesto que como podemos observar en la gráfica inclusive el personal dedicado a la administración de los sistemas de información no tiene una percepción clara de este concepto, teniendo en cuenta que para muchas empresas la información es uno de los activos más importantes en el desarrollo de sus operaciones.

Recomendación.- Planificar estrategias de seguridad de la información que inicien con la concienciación al personal de las empresas acerca de la importancia que representa la información, los controles y procedimientos que rigen la seguridad de la misma.

2.-

Conclusión.- Cuando hemos obtenido el resultado de la consulta sobre si es factible determinar haber sido víctima de un ataque de ingeniería social podemos concluir, en las empresas ecuatorianas no existe el conocimiento adecuado sobre seguridades de la información, la gran mayoría de personas no saben cuando alguien está buscando información para poder realizar un ataque de este tipo y tampoco saben que tipo de información buscan estas personas.

Recomendación.- Capacitar al personal sobre seguridades de la información, prevenirlos sobre los riesgos que corren y darles pautas para evitar que sean víctimas de estos ataques.

3.-

Conclusión.- Una vez obtenidas las respuestas sobre si una llamada telefónica de un jefe o personal de soporte técnico puede ser un ataque de ingeniería social podemos concluir, que en nuestras empresas no existe el conocimiento suficiente sobre las maneras en las que un hacker consigue información y al mismo tiempo tampoco conocemos cual es el valor de la información que tenemos en nuestras manos.

Recomendación.- Educar a las personas sobre los métodos que se usan para obtener cualquier tipo de información, sea esta confidencial o no y las técnicas que utilizadas por la gente interesada en esta información.

4.-

Conclusión.- Después de cuantificar las respuestas sobre la corroboración de la identidad de las personas que realizan una llamada telefónica podemos concluir, que la gente en nuestras empresas no tiene un amplio conocimiento del riesgo que corre y las consecuencias que puede tener el entregar cualquier tipo de información a una persona que no conoce mediante una simple llamada telefónica.

Recomendación.- Concientizar a las personas de la empresa sobre la importancia de resguardar la información de la empresa y de su personal bajo ciertas normas de seguridad y enseñarles el valor y la importancia que tiene la información.

5.-

Conclusión.- Cuando se han obtenido las respuestas sobre la manera en la que son desechados los correos electrónicos con información confidencial podemos concluir, que en nuestras empresas no se tiene una conciencia adecuada sobre el valor que puede tener para un hacker cualquier tipo de información, peor aún si hablamos de información confidencial; la gráfica nos muestra que muy pocas personas trituran esta información, que es la manera adecuada de desechar esto.

Recomendación.- Crear una campaña sobre la manera adecuada de desechar documentos que contengan información valiosa, ya sea para la empresa o para una persona en particular y brindar los medios adecuados para poder realizar esto de la manera apropiada.

6.-

Conclusión.- Al observar las respuestas sobra la consulta acerca del cambio periódico de contraseña podemos concluir, que en las empresas del país en la gran mayoría de casos si se tiene una conciencia adecuada del cambio de contraseñas.

Recomendación.- Mantener como política de seguridad este cambio periódico de contraseñas en todas las aplicaciones y software utilizado en la empresa dentro de cualquier área o departamento.

7.-

Conclusión.- Luego de valorar los resultados de la consulta sobre el tiempo que debe transcurrir para el cambio de contraseña podemos concluir, que en la mayor parte de casos este cambio debe realizarse en un tiempo menor a 3 meses, tiempo adecuado en la mayoría de aplicaciones; sin embargo como se muestra en la gráfica existen casos en los que la contraseña se demora más tiempo en ser cambiada o no se cambia nunca.

Recomendación.- Revisar las políticas del tiempo de cambio de contraseña y regularizar que todos los empleados deben realizar un cambio de contraseña periódico.

8.-

Conclusión.- Una vez evaluadas las respuestas sobre la conciencia que se tiene sobre el impacto que puede traer que no se corrobore cierta información podemos concluir que, no existe un entendimiento adecuado sobre el valor de la información como en muchos otros casos, motivo por el cual la gente no considera importante corroborar cierto tipo de información que puede ser vital para la empresa.

Recomendación.- Educar al personal de la empresa sobre el valor de la información y la seguridad que uno debe mantener con respecto a la misma.

9.-

Conclusión.- Al calcular los resultados de la consulta sobre el tiempo que transcurre para que el personal sea capacitado podemos concluir, que en las empresas de nuestro país no tenemos un pensamiento pro activo en cuanto a capacitación se refiere, el personal tiene una capacitación muy vana y en la mayoría de casos no existen estas capacitaciones.

Recomendación.- Planificar capacitaciones periódicas del personal no solo sobre temas de su área sino también sobre conocimientos sobre información, su importancia y como mantenerla segura.

10.-

Conclusión.- Después de valorar las respuestas obtenidas a la consulta sobre el bloqueo de la terminal cuando se abandona en puesto de trabajo podemos concluir, que en nuestras empresas si existe conciencia sobre la importancia de que su máquina no vaya a ser usada por otras personas en su ausencia, sin embrago, existen casos en los que los empleados no saben li importante que es mantener seguro su puesto de trabajo mientras ellos no se encuentran en el mismo.

Recomendación.- Concientizar al personal sobre la importancia de mantener su información y su equipo resguardado, bloqueándolo cuando uno debe salir de su lugar de trabajo para evitar que otros lo usen en su lugar.

11.-

Conclusión.- Una vez obtenidos los resultados a la consulta sobre si se tiene el nombre de usuario y contraseña anotado en algún lugar visible podemos concluir, que existen un buen conocimiento acerca delo importante que es mantener estos datos como confidenciales, y no en lugares que estén al alcance de cualquier persona.

Recomendación.- Mantener esta conciencia en el personal sobre las seguridades que se deben mantener para resguardar la información personal y empresarial.

12.-

Conclusión.- Al dimensionar las respuestas sobre la consulta de la autenticidad de los remitentes de los correos electrónicos que se reciben diariamente podemos concluir, que en nuestro país no hay el conocimiento adecuado sobre la inseguridad que existen dentro de las redes de comunicación, ya que por medio de un correo electrónico pueden transmitirse muchas herramientas para fugar información.

Recomendación.- Educar al personal sobre la importancia de verificar quien remite los correos electrónico que abren a diario y sobre los peligros y riesgos que existen actualmente y pueden ser transmitidos a través de estos medios.

13.-

Conclusión.- Cuando se obtuvieron los resultados de la consulta sobre la verificación de la autenticidad de un empresa que pide confirmar ciertos datos podemos concluir, que en las empresas ecuatorianas, si se tiene un leve conocimiento sobre el valor de nuestros datos personales, sin embargo, existe gente que entrega sus datos a cualquier persona sin saber quien es ni de que se trata lo que está corroborando.

Recomendación.- Planificar capacitaciones sobre la importancia de la seguridad de la información, el valor que tiene la misma, de que manera puede esta ser robada y utilizada.

14.-

Conclusión.- Después de cuantificar las respuestas de la consulta sobre acceder a cualquier link que contenga un correo electrónico podemos concluir, que en nuestras empresas existe un poco de conciencia sobre el riesgo que existe al acceder en cualquier link que venga insertado en un correo electrónico, pero también hay personas que por simple curiosidad acceden a estos links sin saber que peligros están corriendo dentro de los mismos.

Recomendación.- Enseñar al personal cuales son los riesgos de acceder a cualquier link y la importancia de cuidar su identidad y la información que pueden ingresar en los mismos.

15.-

Conclusión.- Al obtener los resultados sobre la consulta de abrir un documento adjunto de cualquier persona sin verificar el remitente podemos concluir, que dentro de nuestra cultura no esta el verificar quien nos envía un correo electrónico y que es lo que contiene,

por lo que descargamos cualquier tipo de archivo que nos envían sin saber el riesgo que esto trae consigo.

Recomendación.- Capacitar a las personas sobre el riesgo que trae abrir cualquier archivo adjunto sin saber quien lo envía no que contiene, ya que se ponen en riesgo las herramientas de trabajo y la información que puede resultar muy valiosa.

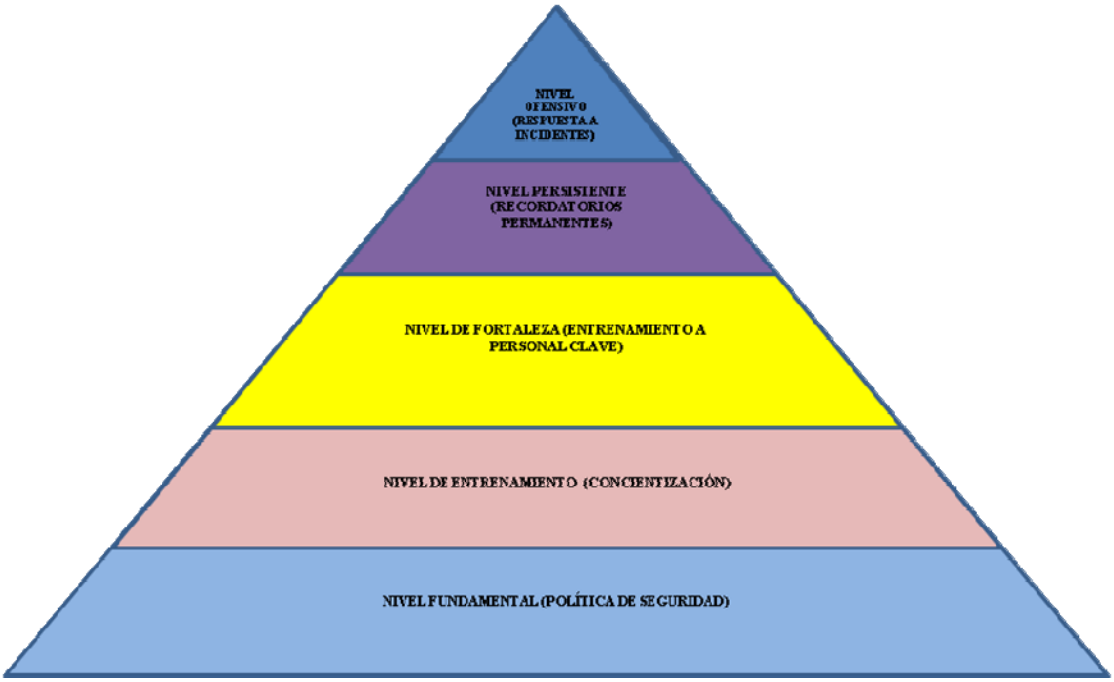
16.-

Conclusión.- Cuando hemos valorado las respuesta de la consulta sobre incluir información sensible en las tarjetas personales de presentación podemos concluir, que en la mayor parte de los casos el personal no incluye información sensible, o ellos no la consideran sensible, sin embargo, existen casos en los que si se incluye este tipo de información.

Recomendación.- Concientizar al personal sobre el valor de nuestra información personal y la manera en la que debemos cuidarla sin regalársela a nadie por el riesgo que podemos correr o en el que podemos poner a la empresa.

CAPITULO VII

7. CONTRAMEDIDAS PARA MITIGAR LOS ATAQUES DE INGENIERÍA SOCIAL



Defensa Multinivel - Creado por: Gabriela Hinojosa

Es posible construir una defensa multinivel contra la ingeniería social, la clave es determinar cuáles son las vulnerabilidades del objetivo y los trucos de los ingenieros sociales y luego defenderse de estos riesgos. La defensa debe tener varias capas de protección de manera que si un hacker pudo penetrar un nivel, debe haber otros niveles en los cuales él o ella puedan ser detenidos. Desde que la ingeniería social ha sido tan exitosa, una estrategia multi-nivel es crítica. En algún punto, la estrategia debe ser más que una defensa porque el ingeniero social que es un depredador, eventualmente va a encontrar un lugar débil.

Dentro de esta defensa multi-nivel se pueden describir varios niveles no solo para prevenir que la ingeniería social entre en la empresa sino que están designados para exponer al hacker. Los niveles son los siguientes:

Nivel Fundamental: Política de Seguridad direccionada a la ingeniería social

Las fortalezas no estarán de pie sin un fundamento fuerte y estable; el fundamento de la seguridad de la información es su política. La política de seguridad define los estándares y niveles de seguridad que va a tener una red, un sistema y/o los usuarios. Este fundamento es aún más crítico cuando la política de seguridad está protegiendo a la red de la ingeniería social.

La política establecida ayuda a los usuarios finales a sentir que deben resistirse a las peticiones de los hackers. Estos usuarios no deben estar en una posición en la que deban considerar si cierta información puede ser llevada o no fuera de la organización. Esto puede ser definido de ante mano por personas que han pensado seriamente en el valor que tiene la información.

La política de seguridad debe direccionar un número de áreas para ser un fundamento para la resistencia contra la ingeniería social. Debe ser una guía sobre los controles de acceso a la información, configuraciones de cuentas, accesos aprobados y cambios de clave. También debe tratar con bloqueos, identificaciones, trituradores de papel y bitácoras de visitantes. La política debe mantener la disciplina dentro de la organización y sobre todo debe ser reforzada en las áreas más sensibles.

El nivel de política de seguridad de defensa en relación con la ingeniería social ayudará a los empleados a defenderse contra los procedimientos sicológicos de autoridad y difusión de responsabilidades. Las políticas tienen un efecto balanceado en la autoridad que una persona puede asumir cuando ellos llaman por teléfono. La política también define la responsabilidad sobre el manejo de la información o los accesos que hay sobre ella de modo que no haya cuestionamientos cuando un empleado bajo su propio riesgo deje salir información privilegiada o de acceso a la misma.

Nivel de Entrenamiento: Entrenamiento para la concienciación sobre seguridad para todos los usuarios.

Una vez que los fundamentos de una política de seguridad han sido establecidos y aprobados, todos los empleados deben ser entrenados y concienciados en cuanto a seguridad se refiere. La política de seguridad proveerá lineamientos para el entrenamiento así como también para tener una motivación para el cumplimiento de esta política. Las políticas que han sido bien pensadas y luego comunicadas a los empleados pueden hacer la diferencia en como los empleados respondan a los diferentes requerimientos.

La concienciación sobre seguridad es bastante complicada, no es suficiente con decirle a la gente, no debes darle tu clave a nadie. En efecto, un hacker conocido, Kevin Mitnick, dijo en una conversación "Yo jamás le he preguntado a nadie su clave." Su meta era mucho más compleja que eso. Era crear un sentido de confianza y luego explotarlo.

Los empleados deben saber qué tipo de información puede usar un ingeniero social y qué tipo de conversaciones son sospechosas, así como también, deben saber cómo identificar información confidencial y deben entender su responsabilidad cuando se trata de protegerla. Deben saber también como decir NO, cuando es apropiado y estar seguros de que tienen el respaldo de su organización cuando esto sucede.

Todos los empleados deben estar conscientes de las señales básicas que están presentes en un ataque de ingeniería social. Entre algunas de las señales que indican que una es sospechosa y debe ser rechazada están, quien llama quiere obtener información de contactos, tiene apuro, solicita nombres, trata de intimidar, tiene mala pronunciación, hace preguntas extrañas y preguntas sobre información que no recuerda. Las personas que están siendo víctimas de un ataque deben estar dispuestas a hacer preguntas a la persona que llama y no revelar información cuando parece que las cosas no están bien; de esta manera los empleados deben estar conscientes de que un buen ingeniero social va a tratar primero de establecer una relación confiable. El ingeniero social luego va a explotar esta relación para obtener toda clase de información de valor. Una gran cantidad de información puede ser obtenida mediante conversaciones casuales como el lenguaje de la compañía, nombres y cargos de personas importantes en la compañía, eventos significantes, la impresión general de la organización, estructura y nombres de servidores importantes.

El entrenamiento debe seguir básicamente las políticas de seguridad pero ahí hay algunos puntos clave que los usuarios deben recordar:

- Mucha gente no valora su información ni el acceso a ella antes de ser hackeado o tener una falla en algún dispositivo. Ellos deben considerar lo que deben hacer si casualmente no pueden acceder a su computadora del todo. Esto debe al menos ayudarles a entender que en lo que ellos han estado trabajando por los últimos cinco años tiene algún valor.
- Los amigos que son hechos por teléfono o por cualquier medio parecido, que pregunten por cosas concernientes a información privilegiada no deben ser amigos del todo. Los ingenieros sociales usualmente buscan ser amigos de sus víctimas antes de preguntarles cualquier cosa. Todos los usuarios deben estar conscientes de que no solo porque alguien parece ser nuestro amigo lo es, esto significa que no pueden darles información privilegiada ni accesos. Dependiendo del valor de la información y el nivel de seguridad que se requiera en la red, los ingenieros sociales van a tomar medidas para convencer al objetivo de que él o ella es su amigo. Esto puede potencialmente tomar lugar en un período de tiempo incluyendo días, semanas o hasta incluso años.
- Aunque muchos hackers nunca van a preguntar por tu clave, otros van a venir con razones muy convincentes por la que un empleado le debe dar su clave a un completo extraño. Desafortunadamente, sin entrenamiento, la gente tiende a dar sus claves sin pensarlo mucho.

  Las claves pueden ser compartidas en un sin número de vías electrónicas. Las páginas web y e-mails pueden dar buenos premios por ingresar en su sitio o a través de una aplicación. Los nombres de usuario y claves que mucha gente usa en estos sitios son los mismos que usan en su red. Si el sitio o aplicación requiere una dirección de correo, el hacker puede también obtener el dominio de la víctima. Los mensajes instantáneos y chats pueden ser también tierra fértil para un ingeniero social cuando se trata de obtener accesos, información o claves de valor.

- Un ingeniero social puede ingresar en un edificio y pretender que él o ella tiene una razón legítima para estar ahí. En muchas oficinas basta con tener el uniforme para ser aceptado. Por eso es importante entrenar a los empleados para no aceptar solo un uniforme como una razón para que alguien esté en algún lugar de la empresa. Los uniformes son baratos y fáciles de adquirir y se debe tener en mente que cualquier información es valiosa para alguien que está tratando de entrar en un

sistema o computadora y treinta segundos de acceso en una computadora pueden comenzar una perfecta ingeniería social inversa.

Nivel de Fortaleza.- Entrenamiento resistente para personal clave

No solo los empleados deben ser entrenados y concienciados sobre seguridad, como parte de una defensa multi-nivel también debe incluir entrenamiento de resistencia para personal clave. El personal clave incluye personal de la mesa de ayuda, servicio al cliente, asistentes de negocio, secretarias, recepcionistas y administradores/ingenieros del sistema.

Básicamente, esto debe incluir a cualquiera que en su trabajo deba ayudar a otros, especialmente público en general y aquellos que trabajan con jerarquización de funciones. Un buen entrenamiento de resistencia ayudará a prevenir que los empleados sean persuadidos para dar información que el hacker pueda necesitar. Estudios recientes han demostrado que el entrenamiento de resistencia puede ser efectivo cuando se trata de endurecer a las personas contra la persuasión. Dentro de las técnicas que se usan para entrenar al personal clave podemos encontrar:

- Inoculación.- La inoculación se produce cuando a los empleados se les ha dado argumentos débiles que serán usados por el ingeniero social. Los empleados pueden estar expuestos a diversos argumentos que un ingeniero social puede usar durante algún tiempo, los que pueden ser refutados con otros argumentos de los empleados. El problema se presenta cuando el entrenador no ha anticipado los argumentos que pueden presentar los ingenieros sociales.
- Alertar.- Alertar es otra técnica que construye resistencia, que ha sido probada por sicólogos sociales. Los sicólogos han probado advirtiendo sobre el tema del contenido que viene en un mensaje y el intento de persuasión que conlleva el mismo. Alertar sobre el contenido causa una gran resistencia, mayor a un intento de prevenir la persuasión.

  La aplicación práctica del entrenamiento de resistencia es prevenir al empleado, de manera que él sepa que el ingeniero social no solo va a tratar de persuadir al objetivo, sino que debe tener claro que los argumentos que él use pueden ser manipulativos, engañosos y no son sinceros. A los empleados se les debe decir que el intento del hacker es criminal y que ellos están intentando robarle. La resistencia

a la persuasión crece si el objetivo tiene mayor conocimiento sobre el mensaje o si el objetivo al menos se percibe a sí mismo como una persona que posee los conocimientos necesarios. La aplicación práctica de estos estudios se da cuando el empleado más informado es el empleado más eficiente en su necesidad de proyectar información y accesos privilegiados, de manera que va a ser menos posible que lo persuadan.

- Chequeo real.- Una de las razones por las que falla el entrenamiento de concienciación de seguridad es que la gente tiende a tener un optimismo no realista sobre sus propias vulnerabilidades. Esta percepción les guía a muchos a ignorar los riesgos legítimos y a fallar en tomar medidas sobre estos riesgos. De cualquier manera, una vez que ellos pasaron por tontos y esto está demostrado, ellos ven que son vulnerables y el entrenamiento es más efectivo.

  Hay tres estaciones para percibir las susceptibilidades al riesgo. La primera es la concienciación, sabiendo que el riesgo está ahí (esto es lo que más detiene el entrenamiento de concienciación.) La segunda es la susceptibilidad general, la cual es creer en la posibilidad del riesgo de otros. La tercera estación es la susceptibilidad personal, la cual es alcanzada cuando se conoce las vulnerabilidades de uno mismo. El entrenamiento de concienciación sobre seguridad y el entrenamiento de resistencia van a tener un valor limitado si uno no alcanza la estación de susceptibilidad personal.

  Disipar la percepción de las vulnerabilidades personales no es un ejercicio cognitivo pero si un ejercicio experimental. Solo diciéndole a un empleado que un ingeniero social puede hacerle parecer un tonto no va a ser suficiente para contar con una actitud de que no es vulnerable.

  Este estudio implica que el entrenamiento de resistencia puede dar idealmente a los participantes la oportunidad de ser vistos como tontos antes de la clase para ganar tanta información como sea posible usando técnicas de ingeniería social de aquellos que van a participar en la clase. Luego el profesor puede dejar a esta persona entrar en la clase y revelarle cuanto ha encontrado en cada miembro de la clase. De esta manera las personas ven que son vulnerables a este tipo de ataques.

  Otra manera de exponer al participante a ver sus vulnerabilidades es tener una aplicación que va a emerger sola y a requerir su nombre de usuario y clave. Puede decir algo como “Su conexión se ha perdido. Por favor ingrese nuevamente su nombre de usuario y contraseña.” Esta aplicación luego retorna un mensaje

dejándole saber que él/ella cayó en su trampa. De otra manera, el entrenamiento de seguridad relacionado con la ingeniería social debe incluir una estrategia permitiéndole al participante ver cuán fácil es para ellos caer en las trampas y verse como bobos. Esta es en realidad la única forma efectiva de decrecer el complejo de invulnerabilidad, así los empleados van a personalizar su entrenamiento y buscar las tácticas de los ingenieros sociales.

Los intentos para entrenar a personas para ser resistentes a los ataques de persuasión probablemente van a ser exitosos hasta cierto punto para que ellos instalen las dos características principales. La primera es que el empleado debe darse cuenta de que la persona que llama está tratando de manipularlo. La segunda característica y más crítica es que los empleados deben darse cuenta de que ellos son personalmente vulnerables a esta manipulación.

Nivel Persistente: Recordatorios permanentes

Una defensa multi-nivel necesitará incluir recordatorios regulares de la necesidad de una conciencia de seguridad. Un disparo a las personas en entrenamiento para resistir la ingeniería social será efectivo por un período muy corto de tiempo. Los recordatorios regulares y creativos son necesarios para mantener a la gente concienciada del peligro que puede acechar en el otro lado del teléfono en una llamada amistosa.

Un buen ejemplo de la necesidad de tener recordatorios regulares es una táctica típica del departamento de policía. Muchos departamentos de policía dan reportes regulares a sus fuerzas de aquellos que fueron asesinados en combate. Esto puede ser un recordatorio constante de que el trabajo es peligroso y de que ellos deben estar en guardia. Esto está hecho de manera que ellos van a estar en guardia contra estos peligros específicos en los que otros oficiales cayeron. De la misma manera, a los empleados se les debe recordar regularmente de la posibilidad de que un hacker atente contra él para robarle información y específicamente informarle sobre cualquier hecho reciente.

Nivel "Te tengo": Ingeniería social un terreno minado (SELM: Social Engineering Land Mines)

La ingeniería social como un terreno minado son trampas que están definidas en el sistema para exponer y detener un ataque. Justo como un terreno minado en un campo de batalla,

esta trampa está definida para “explotar” en la cara de un atacante. Esto destruirá el secreto, tal vez haga que el atacante caiga y detenga el ataque. El SELM alertará a la víctima y a la seguridad de la víctima de que un ataque está en progreso y se debe direccionar a la víctima a una defensa o se debe incrementar la seguridad. Algunas ideas se listan a continuación, pero las ideas realmente están limitadas a la creatividad de los ingenieros en seguridad.

- La justificación de saberlo todo.- Un ingeniero social experimentado no flaquea ante una caminata en una compañía y sin perder tiempo empieza a mirar a su alrededor de su víctima. Una vez que está adentro del edificio, hay continuas posibilidades para él de encontrar información valiosa. Las contraseñas pueden estar escritas a la vista, pueden estar publicadas listas de teléfono de la compañía, información confidencial puede estar alrededor en gavetas, escritorios o impresoras. Cuando hablamos de la justificación de saberlo todo, nos referimos a una persona que hace esto en su negocio para conocer a todos los que están en su piso o caminando en su departamento. Muchos departamentos ya tienen a alguien que hace esto de forma natural. Para ser un SELM, esta persona debe saber de los riesgos de seguridad con la presencia física de un ingeniero social y debe tener el poder para hacer algo rápido para direccionar a un visitante sin escolta.
- Log de seguridad centralizada.- Tener un log centralizado de los eventos de seguridad que es monitoreado por el personal de seguridad de la información puede ayudar a prevenir un ataque efectivo. Cualquier momento en el que se le pida a un empleado algún tipo de información, que redefina una contraseña o incluso cuando tenga una llamada sospechosa, esto debe ser ingresado en el archivo del log central. Si un hacker está obteniendo información por parte del empleado y está usando esta para hablar con otro empleado, los patrones pueden ser notificados en el log. Tan pronto como sea notificado, el personal de seguridad puede tomar acciones para detener el ataque advirtiendo a los empleados sobre el atacante. Los empleados que han sido entrenados y saben que ellos deben reportar todo lo relacionado a la seguridad van a tener menor oportunidad de dar información confidencial sin tomar tiempo para pensar esto primero. Esto ayudará a compensar el gatillo sicológico de reciprocidad así como el ingreso recordará al empleado que hay algo más envuelto y no es una simple relación.

Las actualizaciones que se hacen en el log de seguridad centralizada deben ser monitoreadas en tiempo real, de manera que el SELM puede tomar ventaja de cualquier opción de notificación que la compañía tiene disponible. Las notificaciones de e-mails a cuentas especiales que van a causar que el administrador de seguridad esté en un buscapersonas es una manera de hacer esto. Dependiendo de la frecuencia de ingresos y el tamaño de la empresa, una base de datos dinámica es una buena opción para que funcione mejor.

Para que sea efectivo el SELM con el log central todos los eventos de seguridad deben ser ingresados y los empleados (especialmente los de los puestos de la Mesa de Ayuda y Servicio al Cliente) deben ser evaluados en parte por su adherencia a esta política. El log debe ser centralizado y monitoreado así el atacante no puede rebotar entre diferentes personas en la organización.

- La política de regreso de llamadas.- Un procedimiento bien conocido que puede hacerse para un terreno minado efectivo es una política que requiere que el personal de la Mesa de Ayuda y los administradores de sistemas de regreso de llamadas a cualquiera que haga un requerimiento sobre la renovación de una contraseña o información cuestionable. La llamada de retorno verificará el número de teléfono y debe ser el número de teléfono listado en el directorio para la persona que está llamando. Este es un procedimiento que va a derrotar el truco usando un sistema de PBX y transfiriendo a su alrededor para tratar de hacer algo insospechado para que el objetivo piense que la persona que llama lo está haciendo internamente cuando el distintivo de sonido indica que es una llamada local. Si la persona que llama trata de explicar porqué la llamada de regreso no puede ser hecha o si el número de teléfono no es el número esperado para este empleado, el personal de la Mesa de Ayuda debe tener la libertad de no garantizar los requerimientos y un log de entradas de seguridad debe ser generado.

  En una entrevista, se le preguntó a Kevin Mitnick cual es punto más común en que la compañías caen en su presa; su respuesta fue, dando a alguien de afuera los números internos de la oficina. La gente tiende a ayudar a otras personas que perciben estar dentro de la misma compañía porque la víctima se siente reprimida. El SELM va a prevenir que este punto se haga efectivo.
- Preguntas clave.- Otro SELM es para un número de preguntas que son usadas para verificar la identidad de cualquier persona que esté llamando por información interna o tratando de obtener la renovación de una clave.

La regla de las tres preguntas es una buena opción y puede ser usada pero debe ser definida con todos los empleados. Esta regla provee una lista de preguntas y respuestas que el personal de la Mesa de Ayuda puede usar para verificar la identidad de quien solicita la ayuda. Las preguntas deben ser obvias para el empleado pero no para otros. Un ejemplo podría ser: "¿Cuál era el modelo de tu primer auto?" Cada usuario va a proveer respuestas para la lista de preguntas cuando su cuenta es definida. Las preguntas y respuestas están disponibles para el personal de la Mesa de Ayuda para verificar la identidad de quien está pidiendo la renovación de una contraseña. Una variación de esto podría ser el uso de información que está disponible en la base de datos de autenticación, si es que hay una disponible. De cualquier modo, esta información debe estar publicada y disponible solo para personal autorizado de manera que el hacker no tenga acceso a ella.

Pregunta Falsa: Si ninguno de estos sistemas está definido, una pregunta falsa podría funcionar bien. La pregunta falsa es una pregunta que implica información falsa y le da a la persona que llama la oportunidad de definir lo correcto o construir sobre la información falsa. Esto le puede dar al ingeniero social una oportunidad para dar la mejor respuesta improvisada que el blanco puede reunir. Por supuesto, no importa cuán bien hecho está, el objetivo ya ha sido engatusado. Un ejemplo puede ser: "Oh Sr. Pérez, ¿cómo está su hija?, ¿Está mejor después del accidente?" Si la persona que llama dice, "Mi hija no estuvo en un accidente" o "Yo no tengo una hija", la persona que realiza la llamada ya ha pasado una pequeña prueba. En este punto el empleado debe disculparse y decir que ha cometido un error. De cualquier manera, si la persona del otro lado de la línea comienza a hablar sobre el accidente o le deja al blanco hablar sobre el accidente, luego el hacker estará enganchado. El objetivo enseguida debe notificar a seguridad. Este SELM todavía es útil aunque los números PIN son usados para verificaciones. Si los números PIN son verbales estos pueden ser escuchados. Si ellos son ponchados en el teléfono, ellos pueden ser vistos. Este procedimiento de la ingeniería social del terreno minado es como magia. El que usa esto no puede decir lo que él o ella hizo, no importa cual sea la respuesta. El procedimiento también puede no ser hecho con tanta frecuencia como otros que empiezan a levantarse en lo que se ha hecho. Esto

debe ser un secreto que es guardado entre los empleados de la Mesa de Ayuda y el personal de seguridad apropiado.

- Política del “Por favor espere”.- La literatura sicológica es clara en cuanto a que la gente es más fácil de persuadir para hacer algo cuestionable cuando hay presión, sorpresa o sobrecarga de por medio. Un SELM para vencer debe tener una política que requiere que cualquier llamada sospechosa o cualquier llamada pidiendo una renovación de la contraseña o información privilegiada debe ser puesta en espera. Esto detendrá la acción y le dará al empleado la oportunidad de pensar en algo. Durante la espera, el empleado puede ingresar el requerimiento en el log, discutir el requerimiento con un compañero de trabajo o decidir como verificar la identificación. La clave real aquí es tomar un minuto y procesar la información que está siendo dada para determinar si esta es legítima, necesita más verificaciones o debe ser denegado.

Estas son solo algunas ideas, SELM debe tomar en serio si una postura defensiva va a tener alguna esperanza de ser efectivo. Una defensa estricta sin ninguna ofensiva o espionaje inverso le deja a la red una puerta abierta para cualquier ataque. Si el objetivo no está al menos aprendiendo sobre el atacante mientras es atacado, eventualmente el hacker ganará.

Nivel Ofensivo: Respuesta a incidentes

El nivel final de defensa es la respuesta a incidentes. La necesidad de tener un proceso bien definido empieza tan pronto como él o ella sospecha que algo no está bien. Este proceso debe ir agresivamente después de encontrado el hacker y proactivamente debe informar a las víctimas potenciales.

Si no hay respuesta al incidente, cada empleado que trata con un hacker está peleando una nueva batalla. En el entretiempo el hacker está mejorando al entender las defensas de la organización; los procesos de respuesta a incidentes detienen este proceso. Tan pronto como un ingeniero social es descubierto en cualquier parte de la organización, el ataque se caracteriza y el empleado es alertado sobre el ingeniero social que está ahí y que puede esperar que se presente un encuentro con él.

Es importante tener una persona o departamento trabajando muy cerca y rastreando estos incidentes, así el ataque puede ser caracterizado rápidamente y de manera efectiva. Esta debe ser la misma persona que está observando los logs diarios de cualquiera que esté recibiendo requerimientos sospechosos.

Desde la perspectiva corporativa, hay una necesidad fundamental de un buen entrenamiento. Pero siempre hay la necesidad de algo más: una variedad de formas de recordarle a la gente lo que ha aprendido.

7.1. PROPUESTA DE CAPACITACION PARA DAR A CONOCER LA INGENIERIA SOCIAL

Como ya habíamos mencionado antes entre las cosas más importantes para contrarrestar los ataques de ingeniería social encontramos a la política, la misma que para tener un mayor grado de efectividad, debe contar con la educación como una característica regular. Algunas empresas requieren que todos los empleados revisen las políticas cada año, para que en caso de tener cosas nuevas ellos no tengan problemas con las modificaciones. Todos los empleados nuevos y personas que no son empleados DEBEN ser entrenados tan pronto como ellos comiencen a trabajar en la compañía.

Una parte importante de la estrategia de defensa de la empresa es realizar concienciaciones de los métodos que se han empleado y los comportamientos que han sido fijados por los bandidos para llevar a cabo sus ataques. Educar a los empleados sobre el daño cometido por algunos ladrones, es también un deber.

Debido a que la ingeniería social es una de las herramientas más usadas actualmente por los hackers para conseguir lo que desean de su objetivo, se debe tener en cuenta un plan de

capacitación para que todos los empleados de la empresa, desde los funcionarios de los cargos más altos hasta los funcionarios de los cargos menores, conozcan lo que es la ingeniería social, como se lleva a cabo y cuales son las consecuencias que podría acarrear un ataque de este tipo; por lo que en este subcapítulo se plantea una propuesta de capacitación para dar a conocer la ingeniería social en una empresa.

Primero debemos tener en cuenta que para capacitar a la gente en cuanto al tema de ingeniería social se debe tener en la empresa una política de seguridad para cada una de las áreas, ya que estos ataques pueden darse en cualquiera de ellas, siendo unas más sensibles que otras. Estas políticas deben ser dadas a conocer a todo el personal de la compañía y se debe firmar un acuerdo de que los empleados han leído dicha política y están de acuerdo en que si no se cumple el reglamento serán sancionados de acuerdo al mismo.

Como primer paso en este plan de concienciación las políticas de seguridad de la organización, deben ser escritas y publicadas en la intranet de la compañía. Se debe enviar un e-mail a los jefes de departamento o gerentes informándoles donde pueden encontrar las políticas para que a su vez ellos les informen a sus subalternos que deben ingresar a la Intranet, leer las políticas y firmar el formulario adjunto donde dice que ellos han leído las políticas, las entienden y están conscientes de lo que puede suceder si no se cumplen.

Esto sería el principio ya que el verdadero problema comienza cuando los jefes o gerentes creen que los controles de seguridad están en su sitio simplemente porque están especificados en los estándares.

Hay muchas herramientas que pueden ser usadas en un programa de concienciación de seguridad, las mismas que en cierto grado son efectivas y si son combinadas surgen un mejor efecto, por lo que se debería usar:

- Videos
- Cartas
- Brochures
- Libros
- Posters
- Tazas de café
- Lápices y esferos

- Mouse pads con impresiones
- Protectores de pantalla
- Banner al iniciar sesión en la PC
- Bloques de notas
- Útiles de escritorio
- Camisetas
- Stickers

Se ha comprobado que los banners que se ponen al iniciar sesión, posters y protectores de pantalla presentan problemas cuando no son actualizados de manera constante, por lo que se deberían ser cambiados con cierta frecuencia para llamar la atención de la persona que lo mira. De otra manera son como los avisos que se encuentran a un lado de la vía por la que pasamos conduciendo a diario para ir al trabajo. Si no es cambiada con regularidad, casi no se va a recordar que ahí hay un aviso.

El programa de concienciación debe servir para dar a conocer a los empleados la información de las políticas de seguridad de la organización, para sensibilizarlos sobre los riesgos y pérdidas potenciales y entrenarlos para reconocer las técnicas de ingeniería social. Pero no es suficiente decirles a los usuarios cómo comportarse; ellos deben entender y apreciar las razones que hay detrás de todas estas reglas. Los usuarios, administradores o trabajadores deben formar parte del programa. Un método efectivo que debería usarse es personalizar el asunto de seguridad, enseñarle "qué es lo que hacen, cómo lo hacen y porqué lo hacen" aplicado esto de manera personal, así como para la empresa a la que pertenecen. Una mayor razón para la carencia de concienciación en este tema de la ingeniería social es la falta de comprensión de lo que puede ser perdido a través de estas brechas de seguridad.

De manera que si se educa a los empleados sobre los riesgos de la ingeniería social puede ser la primera línea de defensa, esto puede probar que es una tarea desalentadora. Todos son vulnerables a la explotación mediante ingeniería social pero a nadie le gusta que le digan que es crédulo o algo peor.

Otro punto que debe ser tomado en cuenta ya que es uno de los mejores métodos que se han encontrado y probado para educar a los empleados sobre los riesgos, es tomar historias de ingeniería social sobre eventos actuales y ponerlos en un sitio web interno o usar el e-

mail para dar consejos de seguridad e historias informativas. El guardia de seguridad puede también incorporarse a estas historias en el programa de concienciación que se les da a los empleados. Las historias trabajan como fábulas antiguas, imparten información con algún propósito. Contar historias auténticas de lo que le pasó al “otro pobre hombre” aumenta la resistencia a esta explotación disminuyendo las amenazas, haciendo que el empleado no sea tan vulnerable a la ingeniería social.

El encargado de seguridad debe usar cada oportunidad que se le presente y cada herramienta en su maleta de trucos para asegurarse de que los empleados no solo están conscientes de la necesidad de seguridad sino que entienden porque se requiere esta seguridad.

Los empleados deben tener información sobre a quién llamar cuando surge un evento sospechoso. Ellos deben entender cuál es su responsabilidad al mantener seguros los datos y la infraestructura de la organización. Un programa de entrenamiento de seguridades puede significar la diferencia entre el éxito de un ataque de ingeniería social o el fracaso del mismo. Cuando los empleados están conscientes de la seguridad y lo que la misma significa para ellos y su jefe va a ser menos ofensivo cuando un empleado fiel no tiene la puerta abierta para ellos o pregunta su identidad durante una conversación telefónica. Un programa de concienciación de seguridad apropiado es esencial para combatir los ataques de ingeniería social.

Un punto importante dentro de la capacitación de los empleados, es el que ellos deben conocer quiénes son las autoridades de la empresa y cuáles son sus funciones para evitar la técnica del abuso de autoridad, es decir que solicitan ayuda urgente o información sobre algún procedimiento que debe ser conocido por todos los empleados.

Otra manera muy importante y eficaz para concienciar a los empleados en cuanto a seguridad personal se trata, es a través de los ejemplos de la vida real de compañías que han sido hackeadas o afectadas por medio de información interna o solo por negligencia e ignorancia de parte de un empleado.

Hay organizaciones que contratan personal para llevar a cabo esta tarea. La identidad de las compañías hackeadas se mantiene en secreto por supuesto, en su mayoría por cuestiones de prestigio. Las historias deben ser actualizadas con regularidad, como una vez

al mes. Todo lo que necesita hacer es proveer un vínculo al sitio web donde están publicadas las historias. Alternativamente, para hacer de ésta una experiencia más proactiva, cuando un usuario inicia sesión a diario, puede emerger una ventana con el "ataque" o "defensa" de la historia del día.

Usar pantallas que aparecen de repente cuando la computadora está prendida con un mensaje de seguridad diferente cada día. El mensaje puede ser diseñado de manera que no desaparezca inmediatamente, que requiera que el usuario de un clic que demuestre que él o ella si leyó lo que decía ahí.

Otro punto es comenzar con una serie de recordatorios de seguridad. Los mensajes de recordatorios frecuentes son importantes; un programa de concienciación debe estar siempre en marcha y no detenerse jamás. Los recordatorios no deben ser escritos con las mismas palabras. Estudios han demostrado que estos mensajes son más efectivos cuando varían en las palabras que son usadas o cuando son usados con ejemplos diferentes.

Se pueden usar también pequeños recortes en la cartelera de la compañía. Esto puede no ser una columna completa en el contenido, así una columna sobre seguridad puede ser valiosa. En su lugar, se diseñarían unas dos o tres columnas con un pequeño aviso en el periódico local. En cada emisión de la cartelera, presentar un recordatorio nuevo en forma corta y captando la atención de todas las personas.

Entre las sugerencias para concientizar a los empleados y mantener las políticas de seguridad activas dentro de sus labores diarias, cada cierto tiempo el jefe de seguridad puede tomarse un tiempo no muy largo y realizar un juego de mesa con preguntas acerca de las políticas de seguridad.

También se podría crear un logotipo con algún personaje llamativo que tenga relación con la seguridad y llevar a cabo campañas publicitarias y de concientización de las políticas de seguridad.

7.2. POLÍTICAS DE SEGURIDAD EN LAS ÁREAS MÁS SENSIBLES DE LA EMPRESA FRENTE A LA INGENIERÍA SOCIAL

Para elaborar las políticas necesarias para cada una de las áreas sensibles de una empresa con el fin de mitigar los ataques de ingeniería social, primero se debe conocer que es lo que debe contener dicho documento y qué comprende el mismo.

Una política de seguridad debe ser bien documentada y accesible al mismo tiempo, debe contener estándares y lineamientos que se encuentren asociados a dicho documento y deban ser seguidos para poder cumplir con la política.

La política debe ser claramente documentada en cuanto a los términos legales que contiene, el alcance de la misma y el contenido de cada una de las áreas en las que se aplica.

Como había mencionado al inicio de este capítulo debemos conocer cuál debe ser el contenido de una política de seguridad y en donde debe ser aplicada, por lo que a continuación se explica a que se debe aplicar esta política.

Se deben proteger los datos.-

La política de seguridad de la compañía debe ser muy específica cuando se habla de los guardias de seguridad cuando deben entregar datos valiosos a personal desconocido. Se deben establecer procedimientos exactos para transferir archivos con información sensible. Cuando se deba entregar datos o información sensible, debe existir un procedimiento específico sobre la verificación del perfil de la persona que solicita la información y si es información con un mayor grado de sensibilidad debe existir personal encargado y autorizado para realizar esta entrega.

Para proteger estos datos existen varias técnicas que podrían ser implementados como procedimientos en la política:

- Establecer el debe saber (lo que quiere decir que la persona encargada de proteger la información debe dar su consentimiento para que dicha información sea accedida por la persona que la necesita).
- Guardar un log personal o departamental de las transacciones.
- Mantener una lista del personal que ha sido especialmente entrenado en los procedimientos y quien es confiable para enviar información sensible. Se requiere que solo estas personas pueda enviar información a alguien que no sea parte del grupo de trabajo.
- Si un requerimiento de datos es hecho por escrito (e-mail, fax o correo) hay que tomar otros pasos de seguridad adicionales para verificar que el requerimiento viene de la persona que debería venir.

Cuando se trata el área de las claves o contraseñas se debe considerar.-

Todos los empleados que pueden acceder a cualquier tipo de información sensible actualmente eso significa virtualmente cada empleado que tenga una computadora- necesita entender que actos simples como cambiar de contraseña, aunque sea por un pequeño tiempo, puede guiar a una mayor brecha de seguridad.

El entrenamiento de seguridad debe cumplir el tema de claves y debe enfocarse en la parte de cuándo y cómo cambiar de contraseña. Advertir que constituye una clave aceptable y los desastres de permitir que alguien más intervenga en este proceso. El entrenamiento especialmente necesita cubrir a todos los empleados de ser sospechosos de cualquier requerimiento que involucren sus claves.

En lo superficial esto parece ser un mensaje simple para transmitir a los empleados. No es así, porque apreciar esta idea requiere que los empleados comprendan como un simple acto, el de cambiar una contraseña, puede guiar a un compromiso de seguridad. Se le puede decir a un niño “Mira a los dos lados antes de cruzar la calle,” pero hasta que el niño entienda porqué esto es importante, se debe tratar de que el niño obedezca. Y las reglas para que obedezca son usualmente olvidadas o ignoradas.

Para un ingeniero social, obtener acceso a un sistema puede significar la diferencia entre un ataque exitoso o uno fallido. Una política debe existir para la entrega y creación de contraseñas. Una buena política de contraseñas debe incluir información sobre:

- No compartir contraseñas cuando se le solicita
- No escribir contraseñas
- No usar contraseñas por defecto
- Métodos para identificar usuarios en el reseteo de contraseñas
- Métodos para entrega de contraseñas
- Creación de contraseñas (por ejemplo la longitud mínima de 7 caracteres, que sea alfanumérico, que utilice mayúsculas y minúsculas y no se repitan las últimas 5 claves.)
- Una estación de trabajo segura con una clave de protección para el protector de pantalla cuando se abandona el lugar de trabajo.
- Cambio periódico de contraseñas (cada 60 días por ejemplo)
- Períodos de gracia para la expiración de contraseñas
- Bloqueo cuando falla la autenticación (por ejemplo, la cuenta es bloqueada después de 3 intentos fallidos)
- Estándares para las contraseñas Administrativas y de Sistema

Los empleados deben tomar en cuenta la importancia que conlleva una contraseña fuerte. Usar cualquier palabra que se encuentre en un diccionario o combinación no debe ser permitido, ya que se puede llevar a cabo un ataque de diccionario; es decir, con software especializado se buscan las contraseñas mediante palabras del diccionario y muchas veces funcionan por la falta de cuidado de quien escribe la contraseña. Controlar esto puede ser difícil a medida de que más y más sistemas son implementados, hay más y más contraseñas para recordar. Hay herramientas que pueden ser implementadas, como aplicaciones de cambio de clave, para ayudar a los empleados a escoger una clave apropiada. Tener una contraseña fuerte es extremadamente importante en cualquier ambiente en especial en ambientes en los que se usa tecnologías de una sola firma. Una sola firma le permite al usuario usar una contraseña para entrar a un amplio rango de recursos de red. También se pueden usar estos sistemas para disminuir el estrés de recordar muchas claves, pero esto significa también que hay una sola contraseña que craquear.

Los ingenieros sociales pueden conseguir usualmente las contraseñas simplemente dando un paseo más allá de los espacios de trabajo usando el enfoque físico para obtener información. La invención de las notas post – it han probado ser un dolor de cabeza para los profesionales de seguridad así como también una bendición para los ingenieros

sociales. Es tan común para los individuos escribir sus contraseñas en estos papelitos y pegarlos en el monitor o en otro lugar fácil de encontrar. Otros empleados pueden considerar esconderlo bajo el mouse pad. Una buena política de contraseñas debe requerir que los empleados no escriban sus contraseñas en cualquier lugar y las guarden en lugares visibles o que estén al alcance de cualquier persona; como recomendación se podrían tomar las 6 primeras palabras de una canción y crear con esas iniciales más un par de números y mayúsculas una contraseña fuerte, segura y que no sea palabra de diccionario.

Las políticas fueron creadas para ser seguidas y se debe requerir que el empleado firme un documento en el que conste que estas fueron leídas y comprendidas; tomarse el tiempo necesario para rastrear a los ofensores o ingenieros sociales puede ser costoso y consumir mucho tiempo.

Una política no es buena si no ha sido reforzada, es por esto que el entrenamiento es extremadamente importante y se requiere que exista la seguridad de que esta política se cumple y funciona. Si un empleado en realidad entiende los riesgos involucrados en escribir y pegar por ahí las contraseñas así como el hecho de compartir información sensible, él o ella van a hacer menos este tipo de cosas. Los empleados deben tomar un rol activo en la seguridad de las organizaciones, por lo que un entendimiento del riesgo que conllevan estas cosas y las consecuencias de sus acciones deben ser llevados a casa para ayudar a combatir la ingeniería social.

El personal de la mesa de ayuda o TI de una organización debe seguir una estricta verificación de identidades y una política de entrega de claves. La verificación de la identidad, en este caso, se refiere a la autenticación de una persona que llama para confirmar que realmente es quien dice ser. Los administradores de sistemas necesitan una manera de validar al individuo con el que se están comunicando.

En el mundo actual, reconocer una voz no es un mecanismo suficiente para verificar una identidad. Luego viene el problema de que hay personas que tienen la habilidad de cambiar una contraseña en general. Un empleado de la mesa de ayuda o administrador de sistemas disgustado que puede cambiar claves puede robar información y causar problemas mayores para la organización. Para ayudar a combatir esto, la carga de identificar individuos para reseteos de contraseñas pueden ser cambiados de lugar por alguien de la mesa de ayuda. Con las tecnologías de cambio de contraseñas por uno mismo, un humano no tiene que

validar que otro humano es quien en realidad dice ser. Las tecnologías de respuesta a retos están llegando a ser más y más populares ampliamente usadas a través de los ambientes empresariales. Con la respuesta a retos, se requiere que el usuario conteste una o varias preguntas antes de que se le de la habilidad de cambiar su propia contraseña mediante una interfaz web.

Hay muchas sugerencias sobre la propia entrega de contraseñas. Por ejemplo, algunas organizaciones pueden insistir en que las contraseñas sean entregadas por el mail de la compañía u otro servicio de Courier. Esto significa que las contraseñas son escritas y pueden ser interceptadas. Algunas organizaciones validan al empleado usando identificadores de llamadas. La premisa aquí, en el evento de un cambio de contraseña, es llamar de regreso al individuo al número que aparece en el identificador de llamadas para validar su identidad. Como un método es inseguro, es como que alguien llame desde la estación de trabajo de Danilo y probablemente puede que no sea Danilo. Otras organizaciones validan a los dueños de las cuentas preguntando información personal como el número de seguro social por ejemplo. Esto se relaciona con el almacenamiento de la información del empleado de manera que puede ser accedido por personas que pueden compartir esta información con un atacante o usarla de manera personal. El punto aquí es que muchos métodos de entrega de contraseñas no son 100% seguros. Si las claves son entregadas en papel, de manera electrónica o correo, la identificación de login y la información del sistema nunca debe ser revelada.

Si el correo electrónico no es un medio apropiado de comunicar contraseñas para una compañía, éste puede en su lugar ser usado para dejarle saber al dueño de la cuenta que un requerimiento de contraseña ha sido generado. Por ejemplo, una organización que está usando una aplicación de auto servicio de claves puede tener un sistema en el que envíe automáticamente un e-mail al dueño de la cuenta, o figura autoritaria de una cuenta que indica que la contraseña de una cuenta ha sido cambiada.

El e-mail automático puede incluir la fecha y hora en que el cambio fue realizado y la dirección IP de la máquina en la que el cambio fue hecho. Si la característica de un correo electrónico automático no es adecuada, debe ser permitida una conexión para rastrear los cambios de contraseñas.

Otra consideración cuando se crea un método apropiado de entrega de contraseñas y verificación de identidades es el tipo de cuenta que va a ser actualizada. Una cuenta administrativa para un sistema que contiene abundante información confidencial debe necesitar que se siga un proceso totalmente separado para la entrega, creación y cambio de contraseña.

Por esto es importante crear políticas separadas dependiendo del tipo de cuenta. Debe existir una política separada para cuentas administrativas y cuentas de usuarios. Un estándar de contraseñas separadas puede ser necesitado también por el tipo de cuenta. Una contraseña administrativa o una clave de cuenta de root para un sistema como un firewall puede necesitar ser más larga en caracteres y usar diferentes convenciones de nombre para la identificación del login que la clave de red de un usuario.

Para proteger la red dentro de una política de seguridad.-

Los empleados deben entender que el nombre de un servidor o de la red no es información trivial, pero esto le puede dar al atacante información esencial que le ayude a ganar confianza o encontrar el lugar de la información que desea.

En particular, personas como los administradores de bases de datos que trabajan con software que puede contener información muy sensible, necesitan operar bajo reglas especiales y muy restrictivas sobre la verificación de identidad de las personas que les llama para pedir información o dar avisos.

La gente que regularmente provee cualquier tipo de ayuda con la computadora necesita ser bien entrenada en la clase de requerimientos que debe tener bandera roja, sugiriendo que la persona que llama puede estar tratando de realizar un ataque de ingeniería social.

Defenderse contra la ingeniería social.-

Una buena defensa contra la ingeniería social debe incluir pero no estar limitada a:

- Políticas de contraseñas
- Evaluación de vulnerabilidades
- Clasificación de los datos
- Política de Aceptación de uso

- Chequeos de antecedentes
- Proceso de terminación
- Respuesta ante incidentes
- Seguridad física
- Entrenamiento sobre concienciación de seguridades

Políticas de contraseñas.-

Las políticas de seguridad son indispensables para salvaguardar la información, por lo que deben ser claras, bien planteadas y deben ser conocidas por todo el personal de la empresa; cuando se habla de contraseñas es muy importante mantener una política que sea cumplida por todos los empleados para evitar ser blancos fáciles de un ingeniero social. Estas políticas deben ser leídas y evaluadas constantemente por el personal de seguridad y deben abarcar con todo lo referente a cambio, ingreso y control de claves.

Evaluación de vulnerabilidades.-

Sea este proveído de manera interna o externa, las organizaciones deben implementar una prueba de penetración y vulnerabilidades de manera periódica. Las pruebas usualmente consisten en usar los conocimientos de las herramientas de hackeo y las técnicas comunes de los hackers para comprometer una red. En la ingeniería social es esencial proveer un graven exacto. Desde que un ataque toma ventaja de los empleados, usar ingeniería social como parte de la prueba de penetración puede tener implicaciones legales y debe ser claramente definido y aprobado antes de que ocurra.

Los datos deben ser clasificados de acuerdo a su importancia.-

Desde que los ingenieros sociales usan el conocimiento de otros para tener información, es esencial tener un modelo de clasificación de los datos en lugar de que todos los empleados estén consientes y adheridos a ella. La clasificación de los datos asigna un nivel de sensibilidad a la información de la compañía. Cada nivel de la clasificación de datos incluye diferentes reglas como quien puede ver la información, quien la puede editar y como puede ser compartida. La clasificación de datos también ayuda a asegurarse de la

integridad de los mismos, dependiendo de la clasificación, los documentos deben ser asignados a un dueño o a un responsable de actualizar los documentos.

El siguiente es un ejemplo del modelo de clasificación de datos:

Top Secret: Se refiere a documentos internos altamente sensibles; por ejemplo, adquisiciones, estrategias de inversión, planos o diseños, que pueden dañar seriamente a la organización si esta información fuera perdida o publicada. La información clasificada como Top Secret tiene muchas restricciones de distribución y debe ser protegida en todo momento. La seguridad a este nivel es la más alta posible.

Altamente Confidencial: Es información que al hacerse pública o compartida dentro de la organización puede impedir seriamente las operaciones de la organización y se considera crítico que las operaciones no sigan adelante. La información debe incluir información de cuentas, planes de negocio, información sensible de clientes de solicitantes de bancos y cuentahabientes, etc., historial médico de un paciente e información sensible similar. Esta información no debe ser copiada o removida del control operacional de la empresa sin la autoridad específica. La seguridad a este nivel debe ser bastante alta.

Propietaria: La información de naturaleza propietaria es toda a aquella que comprende; procedimientos, planes de proyecto, diseños y especificaciones que definen la manera en la cual la organización opera. Esta información normalmente es para uso propietario de personal autorizado. La seguridad a este nivel debe ser alta.

Solo para uso interno: Hay información que no es aprobada para la circulación general fuera de la organización, donde puede ser perdida. Esto puede no convenir a la organización o administración pero el desacuerdo es insólito porque puede resultar en pérdidas financieras o serios daños de credibilidad. Los ejemplos pueden incluir, memos internos, minutas de reuniones, reportes de proyectos internos. La seguridad a este nivel está bajo ciertos controles.

Documentos Públicos: La información es de dominio público como: reportes anuales, presentar declaraciones, etc. La seguridad a este nivel es mínima.

Los siguientes términos usados para la seguridad de los datos es: tan alta como sea posible, muy alta, alta, controlada y mínima. La forma en que los datos son protegidos debe estar

basada en el tipo de la clasificación de datos dados. Por esto es importante incluir la clasificación de los datos como parte de una aplicación desarrollada o planeada.

La manera en la que la información top secret es almacenada y protegida variará a cómo estén protegidos los documentos públicos. La información top secret puede ser contenida dentro de una DMZ detrás de firewalls que solo permiten el acceso de clientes específicos al host que contiene los datos, mientras los documentos públicos pueden estar disponibles para cualquier persona que quiera verlos en un sitio web. También es importante tener métodos definidos para la destrucción de los documentos top secret, confidenciales, propietarios e internos.

Hay un modelo de clasificación de datos que puede ser encontrado en el internet, cada uno de estos puede usar lenguajes diferentes para la clasificación de los datos; por ejemplo, usar el término clasificado en lugar de confidencial. SANS ofrece una plantilla para la información sensible la cual puede ser encontrada en: http://www.sans.org/resources/policies/Information_Sensitivity_Policy.pdf

A continuación se describe brevemente la clasificación de SANS:

Toda la información de la empresa se puede clasificar en dos partes:

- Información Pública.- Que ha sido declarada pública y puede ser entregada libremente a cualquier persona sin posibilidad de que pueda causar algún daño.
- Información Confidencial.- Contiene el resto de información, es decir, la que no es pública y es considerada como más sensible que otra y debe ser protegida con mayor sigilo. Esto incluye información como: secretos de negocio, código de programas, potenciales adquisiciones y cualquier otro tipo de información que haga exitosa a la empresa. Dentro de esta clasificación se puede encontrar también información menos crítica como: directorios telefónicos, información general de la empresa, información personal. Existen también acuerdos que se hacen con terceras personas o compañías, dentro de los cuales se debe mantener segura la información proporcionada por estas terceras partes.

SANS dentro de su documento también propone lineamientos de clasificación de los niveles de seguridad, éstos son:

- Sensibilidad mínima.- Información general de la corporación, cierta información personal y técnica.
- Mayor sensibilidad.- Información de negocio, financiera, técnica y más personal.
- Súper sensible.- Secretos de negocio y de marketing de la empresa, operacional, personal, financiera, códigos fuente e información técnica para el éxito del negocio.

Tener un modelo de clasificación de datos ayudará a detener a los ingenieros sociales cuando quieren conseguir información fácilmente.

Toda política debe tener una aceptación de uso:

Una política de aceptación de uso también ayuda al aseguramiento de que los datos confidenciales no sean compartidos y que los sistemas no estén siendo usados de la forma inadecuada. Como toda política, ésta incluye información sobre cómo un sistema de información será usado, esto nos ayuda a asegurarnos de que los sistemas están siendo usados solo para el propósito para el que fueron concebidos. Una política de aceptación de uso debe incluir información como la siguiente:

- Los sistemas de información y recursos de red son provistos solo para uso autorizado
- Proveer credenciales de autenticación para usuarios no autorizados es prohibido
- La información confidencial no debe ser liberada para terceras partes
- Inaceptable uso de e-mail
- Hostigamiento
- Falsificación/distorsión
- Tratar de ganar acceso a recursos no autorizados
- Uso comercial de información de recursos
- Abuso de conectividad a internet
- Denegación de servicios
- Software ilegal o no autorizado
- Uso de redes violando leyes

Se debe realizar un chequeo de los antecedentes para saber con qué personas estamos trabajando y quien está teniendo acceso a nuestra información:

Los ingenieros sociales usarán cualquier método posible para conseguir su objetivo. Si el más común de los ataques de ingeniería social usan intrusos indirectamente, es muy común para un atacante entrar en el interior del objetivo llegando a ser un empleado de la compañía. Los chequeos de antecedentes son importantes para el negocio en general y son una parte esencial de la defensa contra la ingeniería social.

Los chequeos de antecedentes no deben estar limitados a los empleados. A los vendedores y empleados temporales también se les debe aclarar que existen reglas que deben cumplirse antes de ingresar en la red de la compañía de manera remota. Cada compañía debe tener un proceso destacado de chequeo de antecedentes para los empleados internos pero no deben pasar por alto la clase de los chequeos realizados en el personal contratado como servicios de limpieza externos. Simplemente verificando los chequeos de antecedentes que se hayan realizado no es suficiente.

Las organizaciones deben estar conscientes del tipo y exactitud de las comprobaciones de antecedentes realizadas. Un buen chequeo de antecedentes debe incluir:

- Récord Policial
- Resumen de direcciones actual y previas
- Examen de drogas
- Reporte del vehículo que tiene
- Historial de corte civil
- Historial de la corte criminal
- Chequeo de créditos
- Verificación de educación
- Chequeo de referencias personales
- Reporte de compensación del trabajador

Los tipos de chequeos de antecedentes usados variarán de organización a organización así como también dentro de las mismas. Un reporte del vehículo motorizado no debe ser requerido para personas que aplican y no usan los vehículos de la compañía por ejemplo. Tener un chequeo intensivo de antecedentes puede ayudar a asegurar que un individuo con malas intenciones no llegue a ser empleado de la organización, para determinar ataques de ingeniería social.

Esto pasa a través de un proceso de determinación:

Un proceso efectivo de terminación es disuadir a los empleados que han terminado sus labores y no deben usar sus accesos a información y activos fijos para causar daño a la organización. La terminación se refiere a la terminación de accesos a la información y activos físicos, y debe ocurrir cuando un empleado renuncia, es despedido, toma vacaciones o está ausente por algún motivo. Un proceso de terminación de accesos debe incluir el removimiento inmediato de accesos a la red, accesos remotos, acceso a facilidades y todos los accesos a las aplicaciones usadas por los empleados. Cuando un empleado es despedido, su acceso debe ser terminado al mismo tiempo de que él o ella ha dicho que culminan sus funciones de empleado de esa organización.

Sin embargo, las organizaciones deben no desear terminar el acceso antes de que el empleado abandone el edificio, un esfuerzo coordinado necesita estar en medio de los recursos humanos, el administrador de los empleados, personal de seguridad física y seguridad de la información. Cuando un empleado toma un pequeño tiempo para ausentarse debe existir un proceso de terminación de accesos por un período corto. Bloquear cuentas y eliminar cuentas asegura que el empleado no puede causar daños mientras está ausente de su trabajo.

Cuando sucede una remoción de puesto, despido, renuncia o salida temporal de los administradores de sistemas, deben tomarse medidas extras para asegurar que todos los accesos a los sistemas de información sean removidos. Todas las claves de administrador que el empleado conoce o a las que ha tenido acceso deben ser cambiadas inmediatamente. Esto puede requerir que otros administradores paren sus otras actividades, pero es una acción necesaria para ayudar a reducir la probabilidad de un ataque exitoso en la red corporativa. Tener un proceso de terminación en el lugar correcto, que es eficiente, ayudará a las corporaciones a defenderse contra los ataques conducidos por ex - empleados tratando de usar el conocimiento interno.

Se debe tener un plan de respuesta a incidentes:

En el caso desafortunado de que un ataque ocurra, un proceso de respuesta ante incidentes debe tener lugar para ayudar a contener y obtener información sobre el ataque. Un ataque que pasa sin ser notificado debe ser sólo el comienzo de una cadena de ataques. Identificar

y tratar con un ataque de una manera eficiente es importante para deteriorar ataques futuros así como para contener un incidente. Los planes de respuesta ante incidentes variarán ampliamente entre una y otra organización. Es importante tener un proceso de respuesta ante incidentes diseñado específicamente para una organización para tratar con información obtenida y analizada de eventos maliciosos. En el caso de ingeniería social, los empleados deben tener un número telefónico o una persona para contactar inmediatamente después de descubrir que un incidente ha sucedido o está en construcción.

Los empleados deben estar dispuestos a reportar cualquier actividad inusual que encuentre incluyendo llamadas telefónicas.

"En el caso de que los ataques sean detectados y reportados como ataques sistemáticos a través de la organización, el área que se encarga del reporte de incidentes debe estar disponible para determinar cuál es el blanco del atacante de manera que puedan realizarse los esfuerzos necesarios para proteger estos activos."

Cuando nos referimos a las políticas sobre seguridad física, hablamos de:

Tener medidas de seguridad física efectivas, ayudará a minimizar la factibilidad de entrada de un ingeniero social. Hay varios principios básicos que pueden ser implementados, los mismos que pueden reducir grandemente la amenaza de una brecha física, entre los cuales podemos encontrar:

Identificar a las personas que no son empleados:

Debe existir una manera especial de identificar a los individuos que necesitan entrar de manera regular en la compañía. Por ejemplo: los individuos que hacen entregas, vendedores de máquinas en stock, vendedores de ATMs y cualquier forma relacionada por ejemplo personal que recoge objetos para lavado en seco deben tener una única credencial para identificarlos.

Identificación de visitante:

A los visitantes se les debe pedir una identificación física como la cédula o la licencia de conducir así como también se le debe pedir que firme una bitácora donde incluye la hora de entrada, su contacto en la compañía y cuánto tiempo durará la visita. Comparar las

firmas y la cara con el documento, la firma y la foto pueden ayudar al personal de seguridad física a determinar que el individuo es quien dice ser. La cédula o licencia de conducir debe ser fotocopiada y guardada mientras el visitante está en la organización y retenida por un período de tiempo en caso de que un incidente sea reportado después de que el visitante haya salido. Después de la verificación apropiada de la identificación del visitante, se debe crear algún tipo de alarma que se active en el momento en que el visitante indicó que iba a abandonar las instalaciones.

Visitantes escoltados:

Una vez que se le da al visitante la identificación temporal, a ningún visitante se le debe permitir entrar en la organización sin ser asignado primero a un empleado responsable. El visitante debe ser escoltado por ese empleado todo el tiempo en el que se encuentre en el edificio.

Identificaciones Temporales:

Los empleados que han olvidado sus identificaciones deben tener una identificación temporal, el mismo que es asignado una vez que ha sido verificada su identidad. El supervisor del empleado debe ser notificado mediante un e-mail de que una identificación temporal fue asignada a ese empleado por ese día. Todas las identificaciones temporales deben ser registradas y retornadas al final del día, si no es regresada, la identificación debe ser desactivado por los empleados de seguridad física.

Placas de los vehículos:

Si hay un estacionamiento o parqueadero, las placas de todos los vehículos que entran en esta área deben ser registradas por el personal de seguridad.

Basureros:

Los basureros no deben ser accesibles al público. En su lugar deben estar guardados en lugares seguros de manera que estos individuos no busquen a través de éstos para encontrar información confidencial que no fue destruida apropiadamente.

Entrenamiento de concienciación de seguridad:

La parte más importante de una política de seguridad efectiva es asegurarse de que todos los empleados estén conscientes y adheridos a esta. A todos los empleados se les debe pedir que atiendan periódicamente al entrenamiento de concienciación de seguridad. Dependiendo del ambiente, debe ser una buena práctica requerir un entrenamiento de concienciación de seguridad anualmente. Nuevos contratos deben ser requeridos para leer todas las políticas de seguridad así como firmar un documento reconociendo que las han leído, entendido y que están de acuerdo en tolerar las mismas.

Un buen programa de entrenamiento de concienciación de seguridad incluirá información de todas las políticas de seguridad e incluirá información sobre las técnicas de ingeniería social.

CAPITULO VIII

8. CONCLUSIONES Y RECOMENDACIONES

Una vez concluido el trabajo de investigación tanto en la parte teórica como en la parte práctica, se pueden sacar las conclusiones correspondientes y emitir las recomendaciones necesarias en base a lo investigado.

8.1.CONCLUSIONES

- Existe una gran cantidad de información en cuanto a ingeniería social se trata, tanto en el internet como en libros; se han podido analizar los conceptos, las técnicas de ataque, la estructura de un ataque, cual es el comportamiento de un ingeniero social, en donde se puede conseguir información general y confidencial de la víctima, cómo se puede mitigar el riesgo dentro de una empresa frente a estos ataques; pero a pesar de toda esta información, las personas en el Ecuador no tienen una conciencia real de lo que implica un ataque de este tipo, no saben cuál es el valor real de la información y peor aún, no están conscientes de que todas las personas pueden ser consideradas un blanco de ataque para un ingeniero social.

- Una vez conocidos todos estos conceptos se concluyó que, la empresa puede contar con la mayor tecnología, con los últimos equipos del mercado y el mejor software de seguridad, pero si no se crea una conciencia real y no se educa a todos los empleados en el ámbito de seguridades informáticas no se va a mitigar el riesgo de caer en un ataque de ingeniería social; esto es bastante complicado de manejar, debido a que en muchas empresas una sola persona tiene acceso a toda la información sin importar la clasificación que tenga y si no existe la educación adecuada sobre cómo manejar esta información se corre un gran riesgo.

- Dentro de los conceptos de ingeniería social, se pueden encontrar las diferentes técnicas que son utilizadas por los ingenieros sociales el momento de realizar un

ataque, las mismas que son bastante fáciles de usar y generalmente se aprovechan de la ingenuidad o falta de conocimiento de las personas, quienes sin darse cuenta entregan cualquier tipo de información a personal desconocido y no piensan si quiera que esta información puede causar pérdidas desastrosas dentro de la organización o a una persona específica.

- Con el ejemplo práctico que se realizó se pudo concluir que, el personal dentro de las empresas del Ecuador no tiene la educación adecuada en cuanto a seguridades informáticas se trata, no conocen cuales son los riesgos de recibir información como: promociones, premios y propaganda, y no confirmar si esa información es auténtica y no contiene ningún tipo de malware. Se comprobó que con una carta falsa y una "inocente imagen" se puede robar o tener acceso a información confidencial sin que la víctima tenga la menor sospecha de lo que está pasando.

- Después de revisar los resultados obtenidos mediante el ejemplo práctico se puedo concluir que, mediante un programa no muy complicado como es el keylogger, se puede obtener cualquier tipo de información, en este caso se obtuvieron direcciones y contraseñas de correo electrónico, nombres de productos con sus precios y nombres de clientes; todo el software que se utilizó está al lance de cualquier persona, es cuestión simplemente de estudiar la herramienta y sacarle todo el provecho posible.

- Cuando se analizó la parte teórica y la parte práctica del presente trabajo de investigación se pudo concluir que, la falta de políticas de seguridad con lo que a ingeniería social respecta son muy pocas y no se encuentran bien definidas o no abarcan todo lo relevante con respecto a las partes más sensibles de la organización.

- Dentro de las políticas de seguridad, tampoco se encuentra un plan de capacitación para todos los empleados de la empresa, para concientizarles sobre la importancia de mantener una buena seguridad informática y de lo importante que es resguardar la información de cada uno de ellos y de la empresa como tal; no se concientiza al personal en lo que a este tema se refiere, cuando es un tema tan importante que puede traer consecuencias muy graves.

8.2. RECOMENDACIONES

- Se debe crear un plan de capacitación y concientización para todos los empleados, sin importar el cargo que desempeña o el área en la que trabaja, sobre todos los conceptos de ingeniería social, cuáles son las técnicas que usan los ingenieros sociales y qué pasos siguen para poder realizar los ataques. Se debe dar a conocer cuáles son los riesgos que se corre al no saber cuidar la información y al entregarle datos personales e información confidencial a cualquier persona.

- Se debe clasificar la información y se debe mantener un control sobre qué personas tienen acceso a esa información dentro de la compañía, para evitar que una sola persona tenga acceso a toda la información y sea un blanco fácil para un ataque de ingeniería social; dentro de esto también se debe educar al personal sobre el manejo de información confidencial y en caso de ser víctima de un ataque presentar una alerta inmediata al departamento de seguridad sobre la información que fue entregada.

- Dar a conocer al personal todas las técnicas que se usan dentro de ingeniería social y cómo se usan, así como también la manera de reconocer cuando un ingeniero social está poniendo en práctica una de ellas con el personal y cómo evitar caer en las manos del hacker, qué se puede hacer para mitigar el riesgo de ser una víctima de la ingeniería social.

- Concientizar al personal dentro de las empresas sobre lo peligroso que es abrir un link, un archivo adjunto, un archivo desconocido simplemente porque reciben algo que les parece novedoso o interesante; educarles sobre la importancia de siempre verificar si ese archivo o página no es peligroso, si no contiene virus o malware y si es enviado por la persona que dice haberlo enviado. Enseñarles que sus datos son muy importantes y que pueden ser capturados mediante phishing por ejemplo si

entran en una página web falsa o que pueden instalar cualquier cosa en su equipo sin darse cuenta cuando abren cualquier archivo sin verificar lo que contiene.

- Dentro del internet se puede encontrar un sin número de programas que pueden ser muy inocentes pero otros pueden causar daños catastróficos dentro de una empresa, de una computadora personal o pueden robar cualquier tipo de información como en el caso práctico de este trabajo; por lo que, se deben mantener siempre activas las alertas automáticas sobre cualquier tipo de software que sea instalado en la computadora, debe realizarse de forma periódica una revisión de los programas que se tienen instalados en el pc o la portátil de cada empleado, se debe mantener actualizado el antivirus y correr el antivirus al menos una vez al día para evitar que cualquiera de estos programas maliciosos sea instalado en la organización.

- Se deben crear políticas de seguridad que abarquen todo lo concerniente a la ingeniería social, éstas deben ser claras y pueden basarse en cada una de las técnicas usadas por estos atacantes; las políticas deben ser apoyadas por la parte tecnológica ya que hay casos en que las personas olvidan hacer ciertas cosas, como bloquear la máquina, y en este caso se lo podría realizar automáticamente después de un tiempo de inactividad. Así mismo, las políticas deben ser conocidas por todo el personal, deben ser medidas para ver su efectividad y se debe controlar periódicamente que todo el personal de la organización las cumpla.

- Dentro de éstas políticas de seguridad debe constar una en la que se indique que cada cierto tiempo se debe realizar un plan de capacitación y concientización para todos los usuarios de la información y de los sistemas de información, de manera que siempre estén alertas sobre los ataques que se traten de realizar y cada uno de ellos pueda tomar medidas al respecto o sepan exactamente que procedimiento deben seguir ante uno de estos ataques.

BIBLIOGRAFIA

- Beaver Kevin “Hacking for Dummies”. Wiley Publishing, Inc. 2004
- David Gragg, “A Multi-Level Defense Against Social Engineering ” GSEC Option 1version 1.4b, December 2002
- EC-Council “Ethical Hacking” version 5, Module III, Scanning
- EC-Council “Ethical Hacking” version 5, Module IX, Social Engineering
- EC-Council “Ethical Hacking” version 5, Advanced Module, Reverse Engineering
- EC-Council “Case Studies ” Computer Hacking Forensic Investigator
- EC-Council ” ECSA/LPT” Module XXV, Social Engineering Penetration Test
- EC-Council ” ECSA/LPT” Module XXVIII, Physical Security Penetration Test
- EC-Council ” ECSA/LPT” Module XXXV, Ethics of a Licensed Penetration Test
- http://www.gestiopolis.com/canales/demarketing/articulos/61/callcenter.htm
- http://www.alegsa.com.ar/Dic/
- http://www.descargar-antivirus-gratis.com/keylogger.php
- http://www.perantivirus.com/sosvirus/pregunta/ingsocial.htm
- http://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica)
- http://www.rompecadenas.com.ar/ingsocial.htm
- http://www.tp.com.pe/teris/index.php?option=com_content&task=view&id=92&Itemid=42
- http://www.iworld.com.mx/iw_Opinions_read.asp?IWID=64
- http://www.alcancelibre.org/article.php/importancia-seguridad
- http://www.entrebits.cl/foros/zona-hackers-y-seguridad/45-ingenieria-social.html
- http://www.wordreference.com
- Mitnick Kevin & Simon William “The art of Deception”. Kineticstomp.
- David Gragg, “A Multi-Level Defense Against Social Engineering” GSEC Option 1 version 1.4b, December 2002
- http://www.sexovida.com/psicologia/pnl.htm
- http://www.gestiondeventas.com/neurolinguistica.htm
- http://www.definiciones.com.mx/definicion/M/metodologia/
- http://www.wikipedia.org

- Karen J Bannan, Internet World, Jan 1, 2001
- Richard N. Kocsis, “Criminal Profiling” Principles and Practices.
- Kevin D. Mitnick & William L. Simon, “El Arte de la Intrusión”.
- Aaron Dolan, “Social Engineering”

ANEXOS

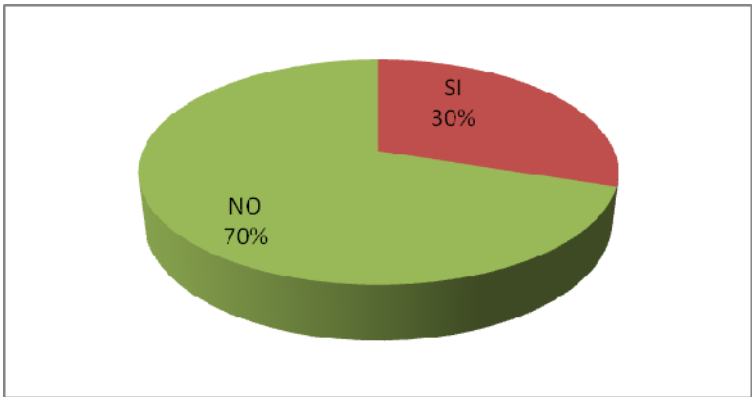
TABULACION

Una vez realizadas las encuestas se realizó la tabulación de las mismas y los resultados se presentan el siguiente orden:

- Encuestas a administradores de sistemas
- Encuestas a Jefes Departamentales
- Encuestas a usuarios finales

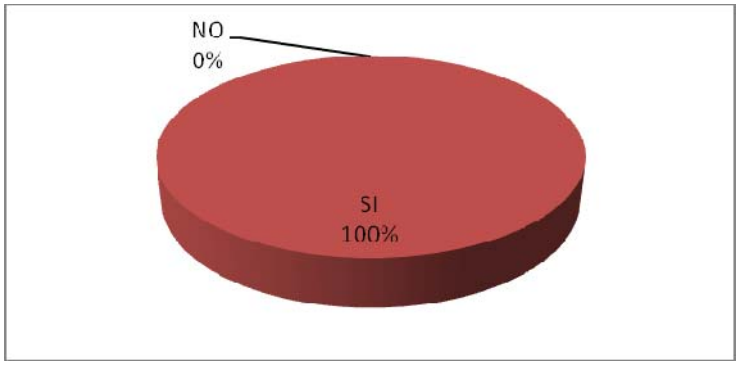
Encuestas a administradores de sistemas

1.- Conoce usted lo que es la Ingeniería Social?

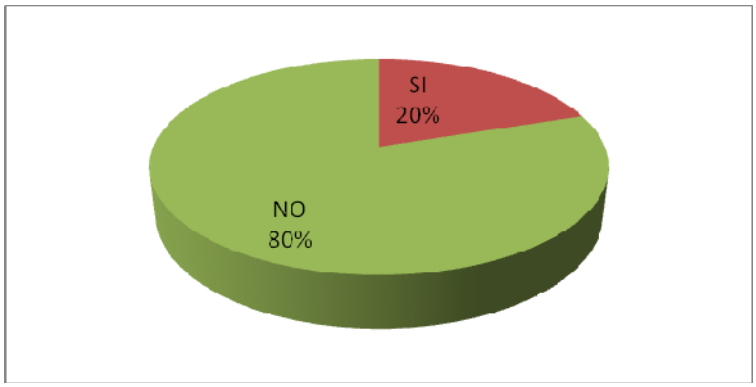


Las personas que respondieron si, coinciden en que es una técnica usada para obtener información confidencial y usarla para obtener algún tipo de beneficio.

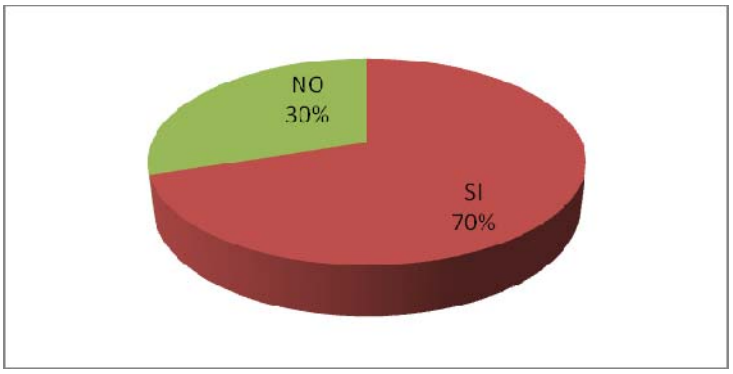
2.- Revisa los antecedentes de las personas que van a trabajar con usted?



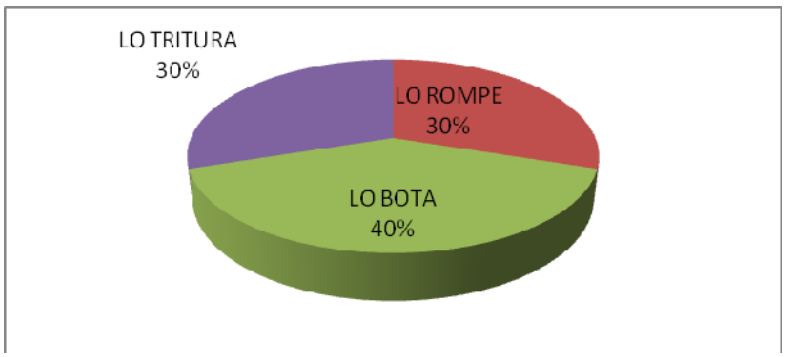
3.-La gente de seguridad de su empresa tiene acceso a información de la infraestructura de la misma?



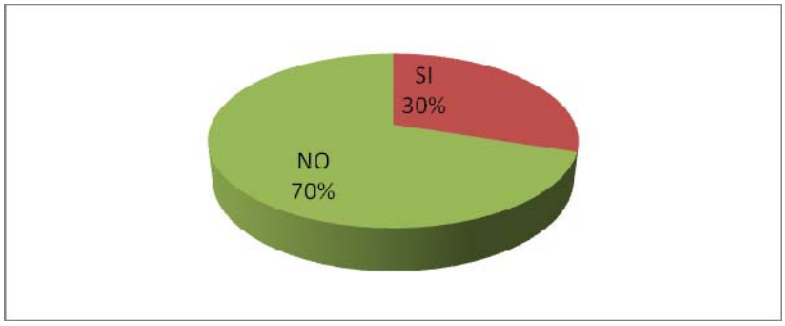
4.- Es pro-activo en cuanto a la capacitación de su personal?



5.- De qué manera desecha un correo electrónico impreso con información confidencial?

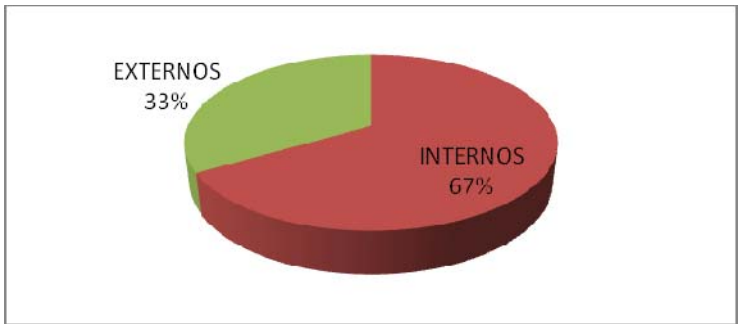


6.- Ha detectado usted ataques de ingeniería social dentro de su empresa?

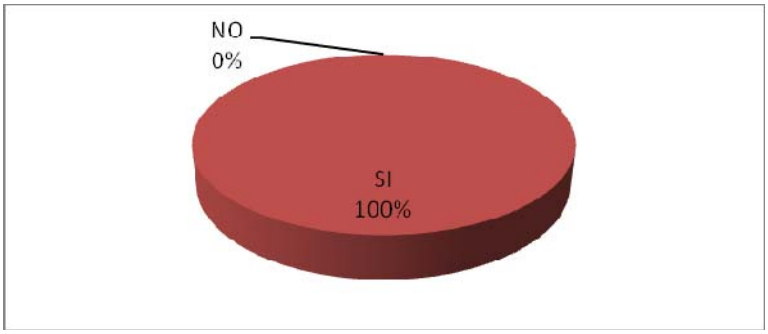


Si la respuesta a esta pregunta fue no, la encuesta finalizó; las personas que respondieron que si terminaron de responder esta encuesta.

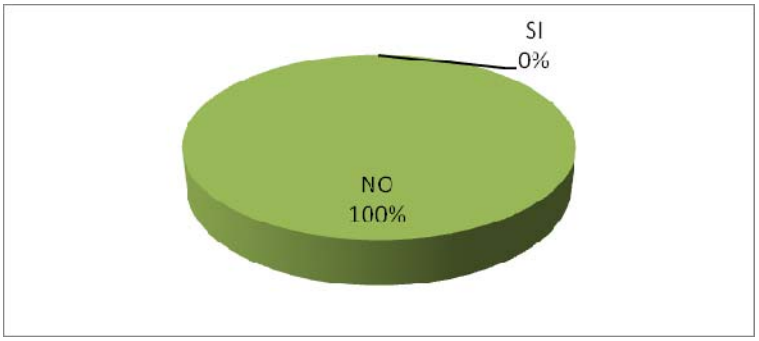
7.- Los ataques detectados dentro de la empresa fueron:



8.- Se realizaron acciones de seguridad para evitar ser víctimas de un nuevo ataque de ingeniería social?



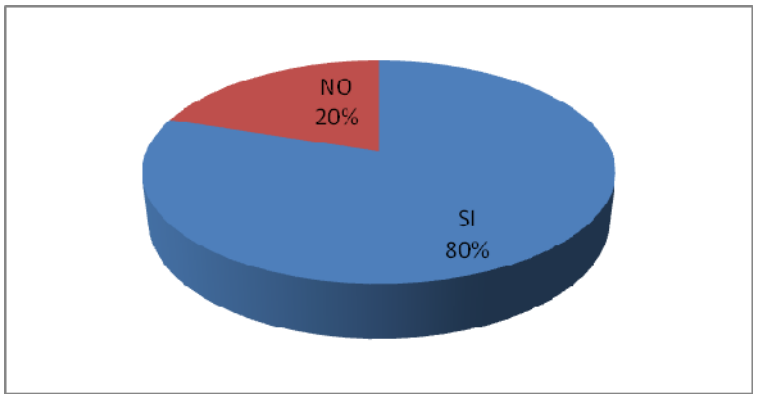
9.- Fue denunciado el ataque de ingeniería social? Porqué?



En su mayoría los ataques no fueron denunciados para que la empresa no perdiera prestigio ni credibilidad.

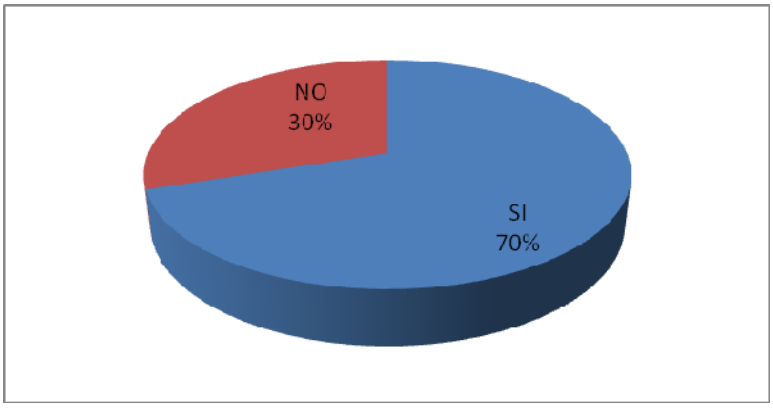
Encuestas a Jefes Departamentales

1.- Sabe usted que es la ingeniería social?

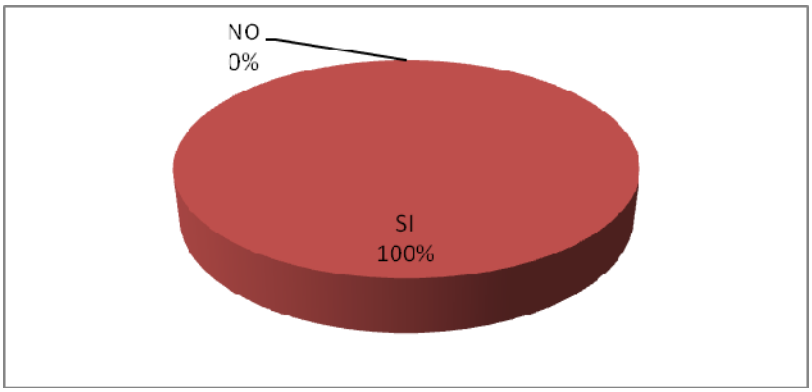


La mayoría de personas encuenstadas dijerojn que la ingeniería social es una técnica o manera de conseguir información confidencial para obtener una ganacia y perjudicar a otros.

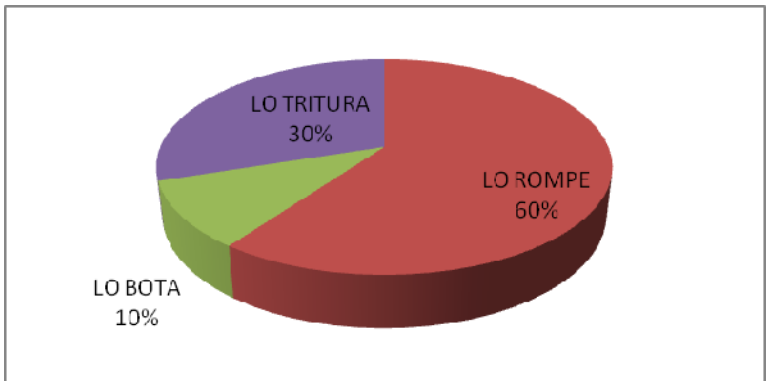
2.- Conoce cómo se lleva a cabo un ataque de ingenería social?



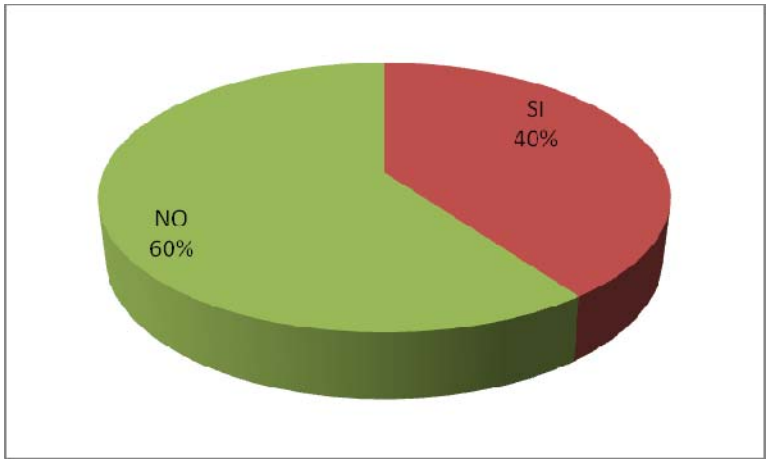
3.- Considera usted, que es fácil obtener información confidencial del personal de una compañía mediante una llamada telefónica, sin necesidad de identificarse?



4.- De qué manera desecha un correo electrónico impreso con información confidencial?

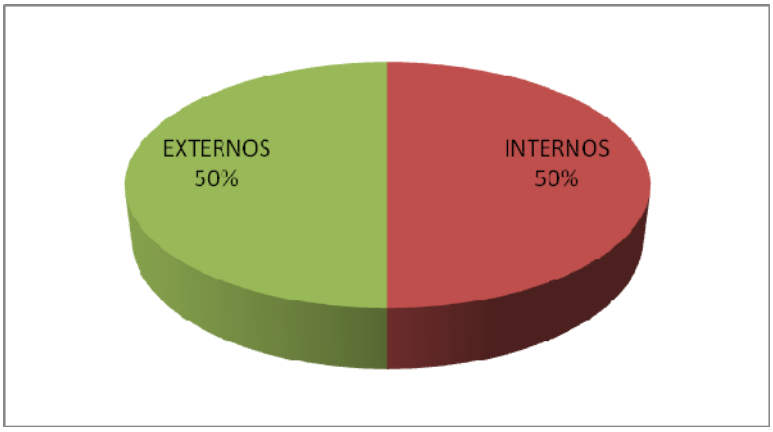


5.- Ha detectado usted ataques de inegniría social dentro de su empresa?

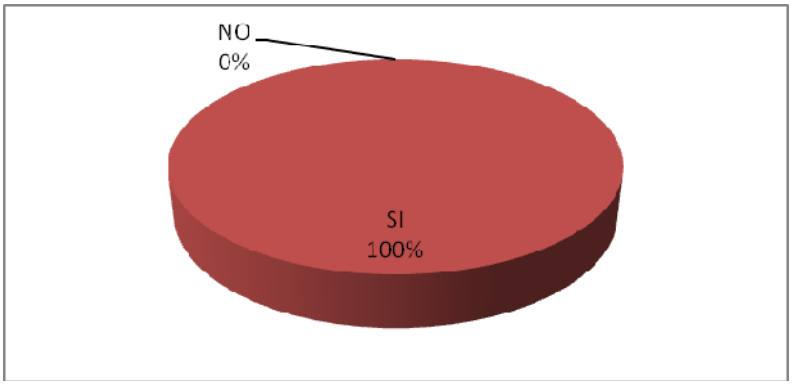


Si la respuesta a esta pregunta fue no, la encuesta finalizó; las otras personas respondieron las encuentas hasta el final.

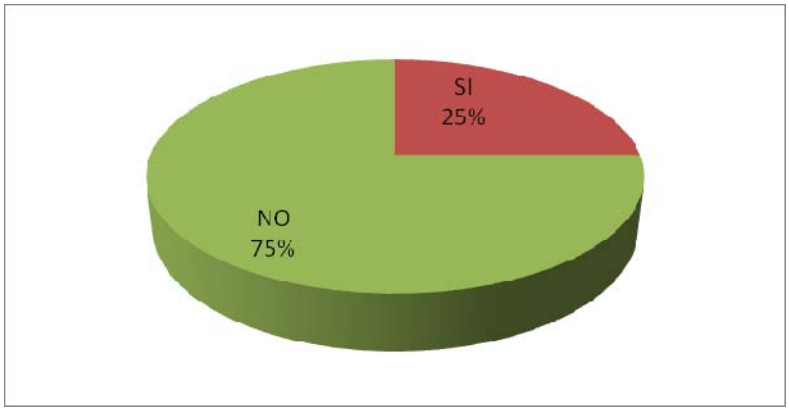
6.- Los ataques detectados dentro de la empresa fueron:



7.- Se realizaron acciones de seguridad para evitar ser víctimas de un nuevo ataque de ingeniería social?



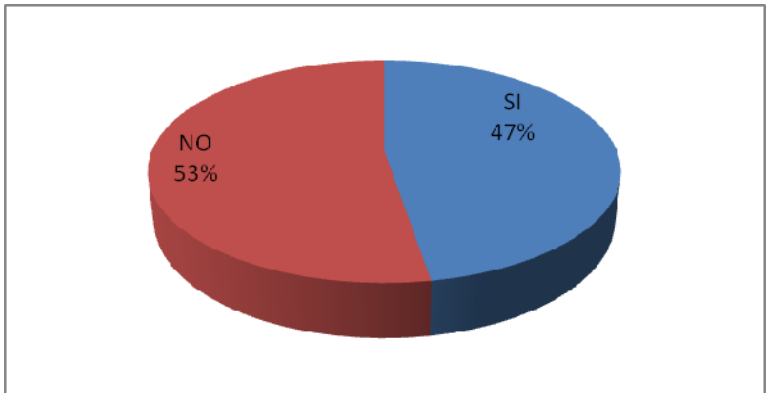
8.- Fue denunciado el ataque de ingeniería social? Porqué?



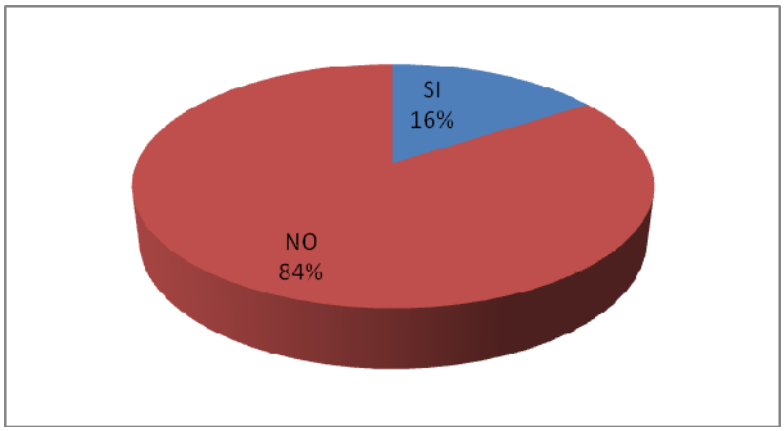
La mayoría de personas no denuncian estos ataques por miedo a perder prestigio y credibilidad de la empresa en si; y la minoría quiere sentar un precedente y tener un registro de cómo se llevó a cabo para no ser víctimas nuevamente.

Encuestas a usuarios finales

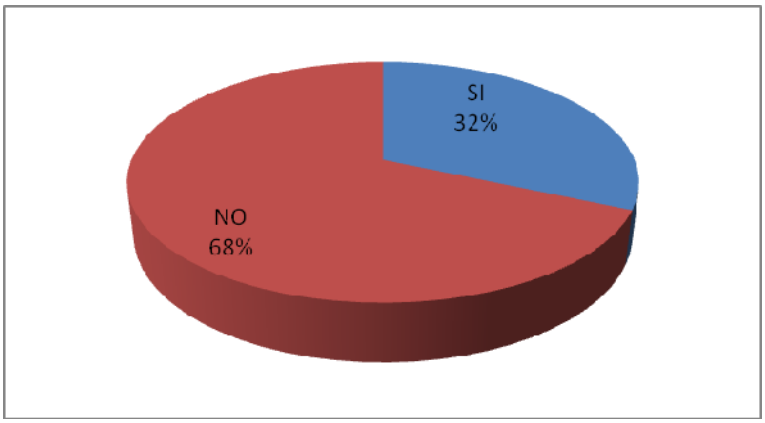
1.- Conoce usted, qué es la ingeniería social?



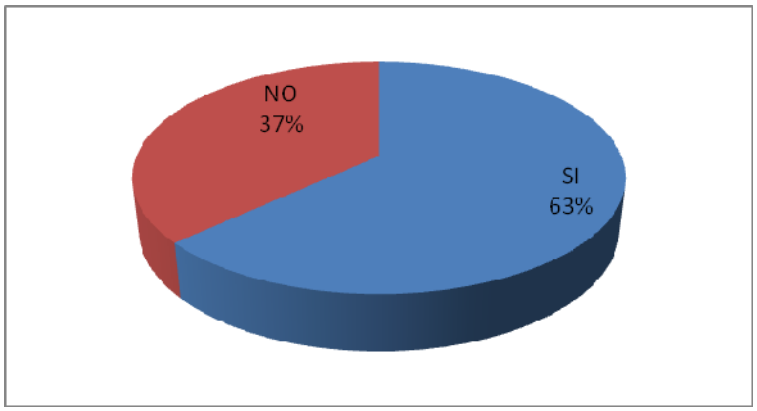
2.- Puede determinar si ha sido víctima de un ataque de ingeniería social?



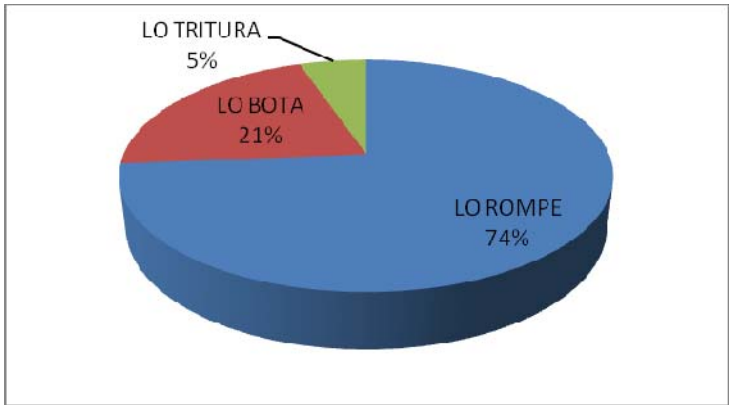
3.- Cree usted que una llamada telefónica de un jefe o del personal de soporte puede ser un ataque de ingeniería social?



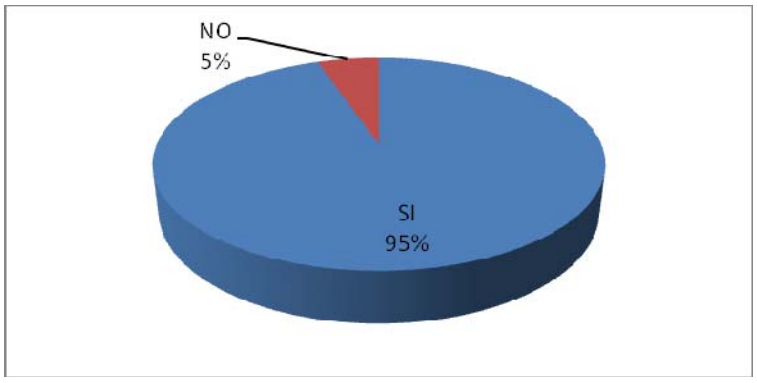
4.- Corrobora usted la identidad de quien realiza una llamada telefónica?



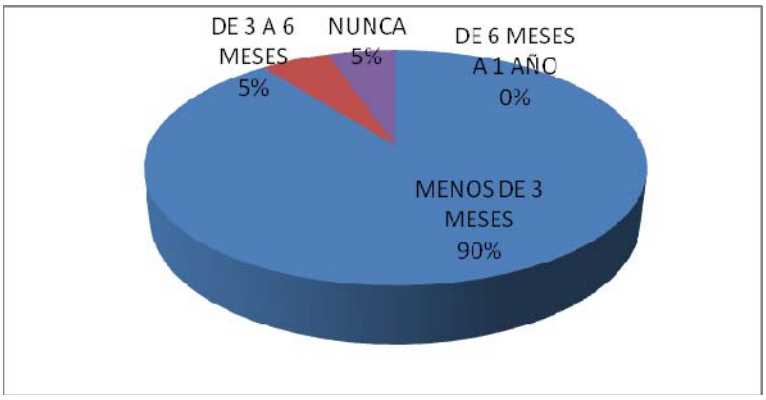
5.- De qué manera desecha usted un correo electrónico impreso con información confidencial?



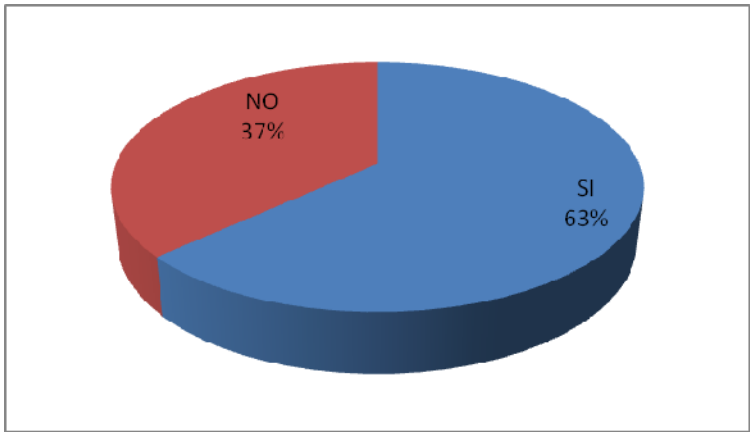
6.- Tiene usted y su compañía políticas de cambio periódico de conttraseña?



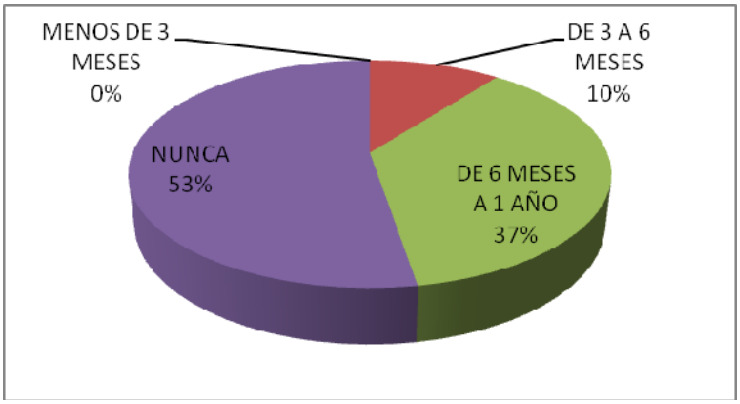
7.- Cuál es el tiempo máximo que debe transcurrir antes de que se le solicite el cambio de su contraseña?



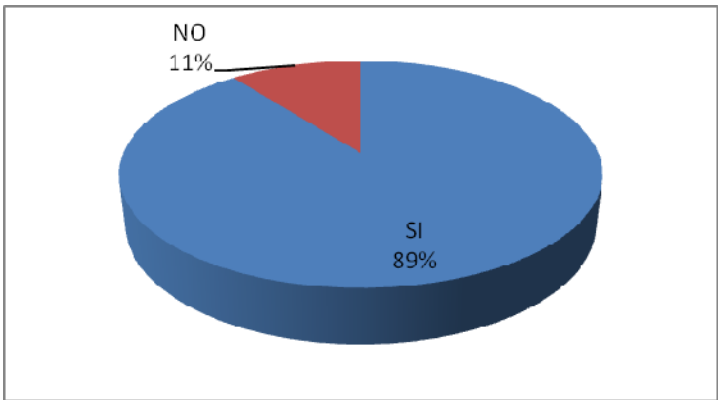
8.- Está usted consiente del impacto que tiene que usted no corrobore cierta información?



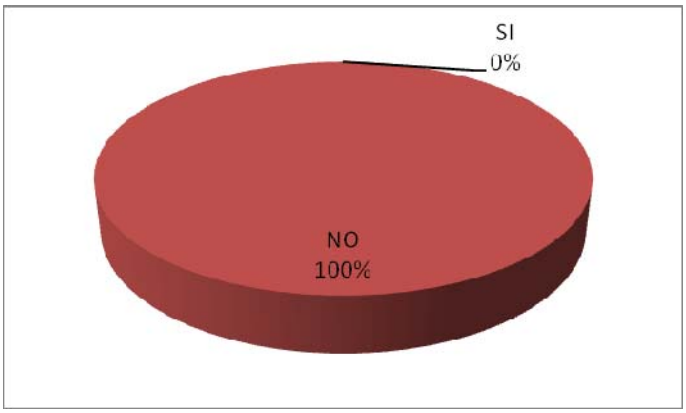
9.- Cada cuanto tiempo la empresa realiza capacitaciones para mejorar el nivel de conocimiento del personal?



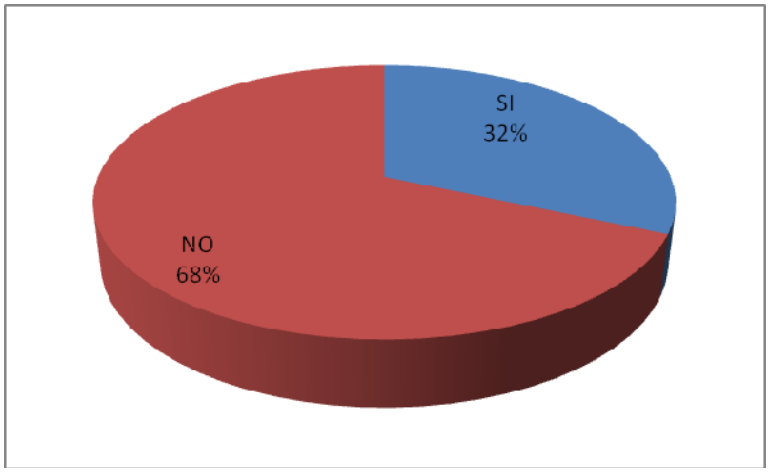
10.- Bloquea usted su terminal cuando sale de su puesto de trabajo?



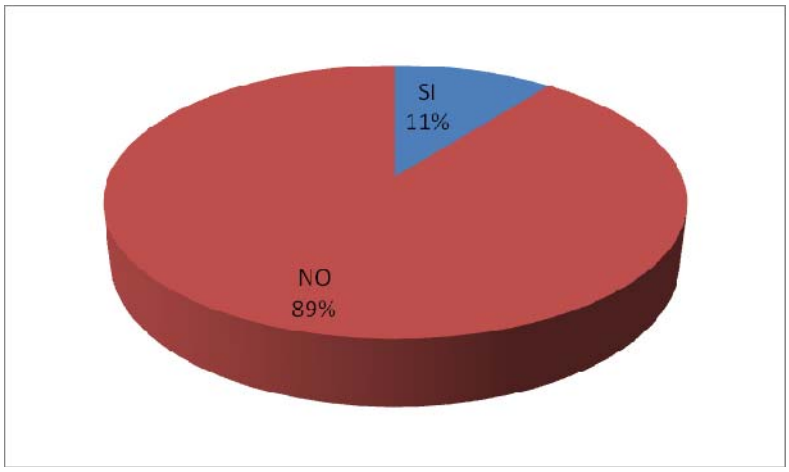
11.- Tiene su nombre y/o password anotado en algún lugar visible?



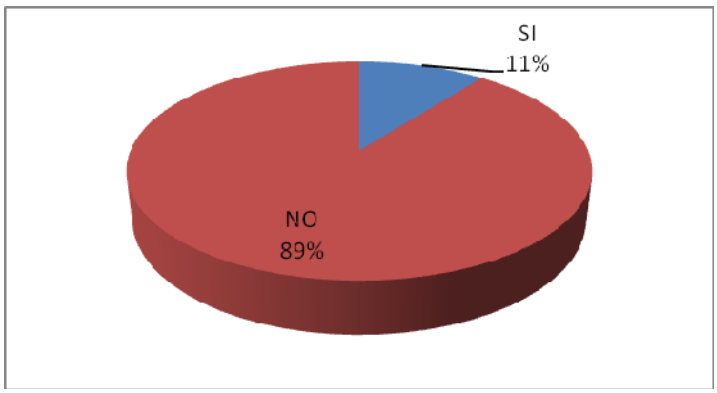
12.- Se asegura usted de la autenticidad de los remitentes de los correos electrónicos que recibe?



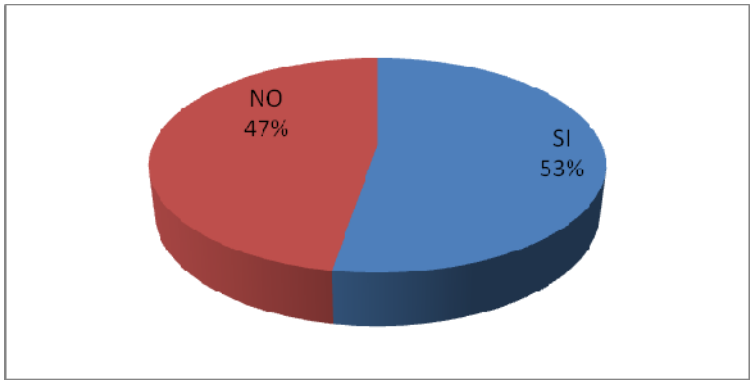
13.- Se asegura usted de que una empresa de servicios es la autora de un correo electrónico de confirmación de datos?



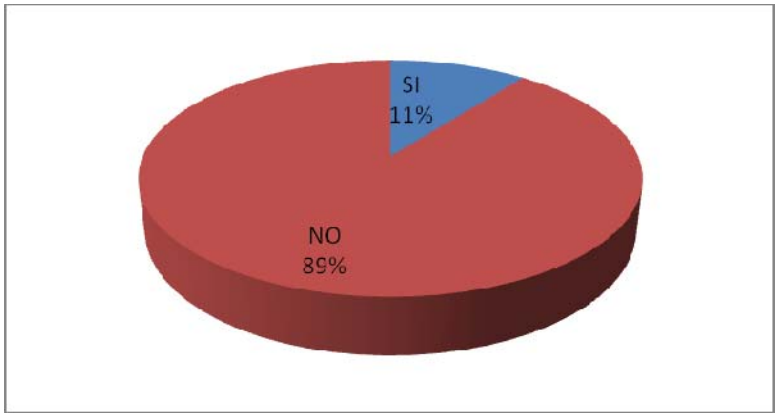
14.- Accede usted a cualquier link que le envían en los correos electrónicos?



15.- Verifica usted el remitente cuando va a abrir algún archivo adjunto a un correo electrónico?



16.- Incluye usted información sensible en sus tarjetas de presentación?



LOGS

xxxxxxxxxxxx @xxxxxx.com xxxxxxxx

xxxxxx@xxxx.xxx.xx pregunta medios de cultivo Estimada xxxx, Por medio de la presente, quiero hacerte una consulta sobre los medios de cultivo que nos pidieron hace unos días para la

Universidad; primero necesito saber si ya regresaron de vacaciones y puedo ya tener una respuesta sobre ellos, segundo quiero saber si recibieron más propuestas sobre ellos porque por ahí me comentaron que tenían una propuesta pero no se si los precios son mejores. Espero que por favor puedas ayudarme con este dato, ya sabes que necesitamos el dato para mejorar las propuestas, avísame cuando puedes para tomarnos un cafecito. Un fuerte abrazo. xxxxxx

Descubraviajes

Agencia de Viajes

Estimada xxxxxxxxx,

Reciba un cordial saludo de quienes formamos la Agencia de Viajes "Descubraviajes", el motivo de la presente es para comunicarle que después de haber realizado un sorteo con una de sus compras en un prestigioso almacén usted se ha hecho acreedora a un viaje por 4 días y 3 tres noches con un acompañante; en el CD que encontrará dentro del sobre podrá escoger el destino al cual le gustaría viajar. Una vez escogido el destino le solicitamos nos envíe un correo de confirmación a la siguiente dirección: descubraviajes@hotmail.com; de igual manera nos puede contactar a este mismo correo en caso de tener alguna pregunta.

El paquete al que usted se ha hecho acreedora, incluye:

- Pasajes para dos personas (ida y vuelta)
- Estadía por 3 noches y 4 días (el hotel depende del destino que elija)
- La estadía incluye desayuno y cena, bebidas gratis durante todo el día y cockteles durante la noche.

Le agradecemos nos confirme los datos que son solicitados en el CD, entre estos se encuentran sus datos personales, los del acompañante y el destino escogido para su viaje.

Felicitaciones y gracias por su colaboración!

Atentamente,

Paola Dávila

Agencia de Viajes Descubraviajes.