UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

ESTUDIO DEL IMPACTO DE LA INGENIERÍA SOCIAL - PHISHING

TESIS PROFESIONAL

PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

PRESENTAN:

DIEGO DANTE GONZÁLEZ JUÁREZ

JOSÉ ANTONIO PEÑA ENRÍQUEZ

DIRECTOR DE TESIS

ING. FRANCISCO JAVIER MONTOYA CERVANTES

Ciudad Universitaria, México, 2012

Dedicatoria

A las personas que me ayudaron a superarme cada día en mis estudios, a mis padres que me dieron su apoyo todo este tiempo incondicionalmente, que me motivaron para seguir adelante y nunca rendirme.
A mi familia y amigos por todo este tiempo que me han acompañado y las alegrías que me han brindado todo este tiempo.

González Juárez Diego Dante

Dedicatoria

Dedicado a las personas que me han apoyado a lo largo de mi formación académica, mis padres y amigos.
A la Facultad de Ingeniería que además de enseñarme los conceptos y definiciones, me enseño la importancia del razonamiento.

Peña Enríquez José Antonio

AGRADECIMIENTOS

A nuestro director de tesis ING. FRANCISCO JAVIER MONTOYA CERVANTES por su apoyo incondicional para con nosotros, sus valiosos consejos, criticas, aportes y comentarios que nos brindo durante todo el desarrollo de nuestra tesis.

A nuestros compañeros por todos estos años de compañía que nos han brindado:

Andrea Pliego, Carolina Reyes, Mariana Dolores, Paola Ivett, Gabriela Oliva, Miriam Alejandra, Viridiana Cuellar, Edgar Mondragón, Luis Ernesto, Josafat García, Ing. Diego Monroy, Aldo Leandro, Everardo López, Javier Vega, Joari Martínez, Luis Enrique, Ricardo Andrade, Ricardo Hernández, Miguel López, Luis Ángel, Raúl Isaac, Pablo Erico.

A nuestros profesores por ser comprensivos, brindarnos sus conocimientos para poder formarnos como ingenieros:

Ing. ORLANDO ZALDIVAR, Ing. M.I NORMA ELBA CHÁVEZ, M.A. GAYOSSO ESCAMILLA HILARIA NELLY, Ing. GABRIELA CAMACHO VILLA SEÑOR, Ma. JAQUELINA LÓPEZ BARRIENTOS, Ing. MA. EUGENIA MACÍAS RÍOS, Ing. ARREDONDO GARZA JOSÉ ANTONIO DE JESÚS, Ing. RAMÍREZ TAQUEZ JOEL.

Por último ofrecemos una disculpa a todas las personas que nos han apoyado todo este tiempo y que no pudimos recordar.

Índice

En la actualidad es muy común ver en centros comerciales, escuelas o parques públicos, a personas utilizando sus dispositivos móviles para consultar su correo electrónico, realizar pagos bancarios por medio de la banca móvil o actualizando sus perfiles en las distintas redes sociales; esto solo por citar algunos ejemplos de una infinidad de operaciones que se pueden realizar gracias al avance de tecnologías de comunicación y el desarrollo de dispositivos móviles.

En estos días, donde empresas y personas dependen tanto de la tecnología, el término de "valor de la información" y la "seguridad informática" han tomado gran importancia sobretodo empresas que buscan cuidar sus activos de información. La seguridad informática se encarga de proteger los sistemas computacionales y todo lo que se relaciona al sistema (como información almacenada, bases de datos, software, hardware, etc.) por medio de la creación e implementación de estándares, protocolos y herramientas de seguridad además de ampararse con las leyes propias de cada país con respecto a la protección de datos personales.

También el factor humano es una parte esencial del juego de seguridad. No existe un sistema informático que no dependa de algún dato ingresado por un operador humano. Esto significa que esta debilidad de seguridad es universal, independiente de plataforma, el software, red o edad de equipo. Existe una frase popular que dice que la única computadora segura es la que se encuentra apagada y desenchufada.

Sin embargo, como se ha repetido a lo largo de la historia, con el desarrollo de nuevas herramientas de tecnología y de comunicación, surgen personas que buscan explotar las vulnerabilidades de estas nuevas tecnologías, pero sobre todo se enfocan en engañar al eslabón más débil de una cadena de seguridad: el usuario.

Es importante conocer que organismos protegen la integridad de nuestros datos personales que se entregan tanto a particulares como al gobierno, en el capítulo 1 se verán los principales organismos encargados para este propósito y la capacidad que tienen para resolver problemas de esta índole.

En los capítulos 2 y 3 se observaran las prácticas más comunes de *Phishing*, así como la frecuencia de los delitos informáticos y la forma más común en que se propagan.

En el capítulo 4 se elaboran una serie de recomendaciones para la seguridad tanto para las empresas como para los usuarios.

Por último se espera que la presente investigación sea de gran ayuda para mantener informado a las personas y tengan una serie de precauciones simples, con las cuales se evitaran en su mayoría, los ataques más comunes de *Phishing*.

OBJETIVO GENERAL:

Investigación sobre la importancia que ha tomado la Ingeniería Social conforme al desarrollo de nuevas tecnologías de comunicación, en caso particular la técnica conocida como *Phishing*. Presentar un panorama actual del fenómeno de *Phishing* y dar a conocer las legislaciones del Gobierno Mexicano referentes hacia la protección de datos personales.

Objetivos particulares:

- Conocer acerca de las prácticas de *phishing* desde una perspectiva social y tecnológica e identificar las consecuencias derivadas de su práctica.
- Dar a conocer la frecuencia de los delitos informáticos (robo de información sensible, robo de identidad, fraude económico).
- Dar a conocer las formas de ataque más comunes asi como los medios donde se propaga.
- Dar a conocer las Instituciones encargadas de proteger la legalidad en referencia a la protección de datos personales.
- Crear un material bibliográfico para que sirva de base para otras prácticas del estudio de la Ingenieria Social.
- Dar a conocer las formas de prevenir ésta práctica.

CAPÍTULO I

INTRODUCCIÓN A LA INGENIERÍA SOCIAL

Este capítulo mostrara los conceptos necesarios para la comprensión del proyecto.

CAPÍTULO I INTRODUCCIÓN A LA INGENIERÍA SOCIAL

1.1- Que es la Ingeniería Social

El conjunto de técnicas destinadas a explotar las vulnerabilidades de seguridad de un sistema recibe el nombre de Ingeniería Social, el Ingeniero Social intenta persuadir y manipular a una persona para obtener información personal sensible o información sobre las empresas donde trabajan.

Los objetivos de la Ingeniería Social en general es ganar el acceso no autorizado a sistemas o a redes de información esto con el fin de cometer fraude, entrometerse en las redes, realizar espionaje industrial, robo de información, etc. Contrariamente a la creencia popular, es a menudo más fácil de utilizar a las personas, que explotar vulnerabilidades o malas implementaciones de un sistema y a su vez, toma más esfuerzo educar a los usuarios para que puedan prevenirse y descubrir un posible ataque de parte de un ingeniero social que mejorar las políticas de seguridad de un sistema.

Cabe resaltar que estas prácticas no nacen con la creación y desarrollo de la computación, si no que éstas son versiones de prácticas ilegales ya existentes, se tiene casos de personas realizando este tipo de estafas aprovechando medios de comunicación tan viejos como el correo tradicional; sin embargo las facilidades que ofrecen los nuevos dispositivos han conducido al desarrollo de métodos mucho más elaborados y difíciles de detectar (por ejemplo es fácil identificar si la letra de una carta no corresponde al supuesto remitente cosa imposible de hacer con el correo electrónico) y por lo tanto más eficientes en cumplir su objetivo. El usuario se enfrenta diariamente a páginas Web falsas, publicidad engañosa (prometiendo productos o servicios muy interesantes o provocativos), programas o aplicaciones engañosas o simplemente personas que buscan obtener información en cuartos de chat o por las redes sociales.

La mayoría de las personas son lo suficientemente ilusas como para dar su información a un extraño a cambio de recibir algún beneficio o sin darse cuenta suministran su información, como cuando se arroja un papel a la basura con su contraseña escrita, dejando un papel con su contraseña debajo del teclado o utilizando contraseñas fáciles de descifrar como el nombre de la persona o su fecha de cumpleaños, etc.

Los ejemplos anteriores tal vez parezcan burdos y tontos para usuarios expertos como administradores, técnicos, analistas de sistemas, etc.
Sin embargo las victimas que busca el Ingeniero Social son personas con bajo nivel de conocimiento en sistemas o personas que presentan poco interés en la protección de sus datos o de la empresa donde laboran; por lo general las víctimas de estos ataques son los guardias, personal de limpieza y de mantenimiento y recepcionistas con acceso a computadora, básicamente personas que no conocen el razonamiento de un Ingeniero Social.

A partir de los ejemplos se puede comprobar que la Ingeniería Social puede tomar distintas formas, desde las más amigables hasta como las más violentas, a continuación se presentan algunas de las facetas que puede tomar el Ingeniero Social:

- *Hackers*: Es una persona que busca como explotar vulnerabilidades en el *software* de un sistema para perjudicar un organismo o por simple logro personal, sin embargo con el avance y el endurecimiento de la protección de *software*, los *hackers* están recurriendo a técnicas de Ingeniería Social. A menudo usando una mezcla de *hardware* y habilidades personales, los hackers están utilizando la Ingeniería Social en los ataques más importantes, así como en infracciones leves en todo el mundo.

- *Espías*: Los espías son el ejemplo máximo de lo que es la Ingeniería Social, a menudo, el espía emplea todos los aspectos del sistema de Ingeniería Social. A los espías de todo el mundo se les enseñan los diferentes métodos de "engañar" a sus víctimas haciéndoles creer que son alguien o algo que no lo son. Muchas veces los espías también se basan en la credibilidad de saber un poco o incluso mucho acerca de la empresa o del gobierno donde están tratando.

- *Empleados descontentos*: Se puede definir como aquel empleado que sostiene una relación de confrontación con su empleador. Esto a menudo puede ser una situación de un solo lado, porque el empleado por lo general trata de ocultar su nivel de desagrado para no poner en riesgo su empleo. Sin embargo, entre más descontento se encuentre el empleado, más fácil será para el justificar actos de robo, vandalismo y otros crímenes.

- *Pruebas de penetración*: Son personas que utilizan las herramientas de un *hacker* pero que, usualmente, no usan la información obtenida para beneficio personal o causar daños, su meta es identificar fallas de seguridad.

- *Ladrones de identidad*: El robo de identidad consiste en usar la información como el nombre de una persona, número de cuenta bancaria, dirección, fecha de nacimiento, número de seguro social, etc. sin que el propietario de la información tenga conocimiento. Este delito puede variar desde ponerse un uniforme para hacerse pasar por alguien hasta estafas más elaboradas como el *Phishing*.

- *Vendedores*: Gurúes de las ventas dicen que un buen vendedor no manipula a la gente, pero utiliza sus habilidades para saber qué necesidades tienen las personas y luego ve si lo puede llenar. Para las ventas se necesitan habilidades tales como la recopilación de información, la influencia y principios psicológicos.

- *Gobiernos*: No muy a menudo son vistos como Ingenieros Sociales, los gobiernos utilizan la Ingeniería Social para controlar los mensajes que emiten, así como las personas que gobiernan. Muchos gobiernos utilizan la prueba social, la autoridad, y la falta de información para asegurarse de que sus asuntos están bajo control.

1.2- Formas de Ingeniería Social

Existen diferentes métodos para llevar a cabo la Ingeniería Social, es muy importante tener en cuenta cuales son cada uno de ellos para evitar ser víctima de esta práctica, como se ha explicado con anterioridad cualquiera persona puede caer en este tipo de prácticas por eso se mencionarán a continuación las formas más conocidas:

- *Simple Embaucamiento*: Esa es una estafa de las que más creatividad se necesita ya que consiste engañar a la victima dándole a creer que recibirá grandes beneficios por proporcionar información, realizar acciones como sustraer información de la empresa donde trabaja o realizar una inversión.

- *Phishing*: Como se sabe *Phishing* se deriva del vocablo inglés "*fishing*" o pesca, por la metáfora de "pescar" víctimas incautas a través de señuelos. Este término informático se refiere a un delito dentro del ámbito de las estafas, éste se comete al intentar adquirir información confidencial de forma fraudulenta, puede ser obtener una contraseña o información detallada sobre tarjetas de crédito, etc. El estafador, conocido como *phisher*, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas, igual puede ser una persona de confianza con la que se tiene contacto.

- *Spear Phishing*: El *S*pear *Phishing* es una variante del *Phishing*, esta se traduce como "pesca de arpón" porque es un ataque de *Phishing* dirigido a un objetivo específico. Los timadores de S*pear Phishing* envían mensajes de correo electrónico que parecen auténticos a todos los empleados o miembros de una determinada empresa, organismo, organización o grupo.

- *Envió de troyanos y/o keylogger*: Se envía un correo electrónico a la víctima potencial con un *troyano* adjunto que por lo general es un *keylogger*, un *keylogger* es una programa que registra las pulsaciones del teclado para memorizarlas en un archivo, estos programas se envían a una persona que le sea familiar o simplemente con un interesante título al destinatario como "es divertido, pruébalo", etc. El troyano no es más que un *programa malicioso* capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información o controlar remotamente a la máquina anfitriona.

- *Recolección de hábitos de víctimas potenciales*: Este método se basa en la creación de perfiles ficticios e infiltrarse en redes sociales o en servicios de mensajería, de esta forma se puede recolectar información acerca de los hábitos de las víctimas potenciales. Para las redes sociales solo basta con echar un vistazo en fotos de viajes o la información personal que se proporciona, de la misma forma si se puede tener comunicación basta con que se entable una relación para poder obtener la información que se necesita.

- *Trashing* (recolección de basura): Revisar los desperdicios y la basura es otro método popular que aplica la Ingeniería Social, una gran cantidad de información puede ser recogida desde los recolectores de basura de las empresas. Algunos de esos artículos echados en la basura que pueden representar una potencial fuga de información son, libretas telefónicas, organigramas, memorandas, manuales de procedimientos, calendarios, manuales de operación de sistemas, cuentas de usuarios y sus contraseñas, etc.

- *Vishing*: Se basa en técnicas de *Phishing* aplicadas sobre el protocolo *VoIP* para obtener información de una persona que pudiera ser estafada. Los cibercriminales por lo general utilizan un sistema de mensajes pregrabados o a personas que llaman para solicitar, en muchos casos, información financiera personal. Una llamada para avisar que su tarjeta se usa sin tu consentimiento puede significar una estafa, por ejemplo al avisarle que se realizaron cargos no autorizados y que se necesita corroborar sus datos, cuando se marca contesta una grabación pidiendo el número de la tarjeta, fecha de vencimiento y código de seguridad.

1.3- Importancia del estudio de la Ingeniería Social

Como ya se mencionó anteriormente, la Ingeniería Social no es un fenómeno nuevo, siempre está en constante evolución paralelamente con las nuevas tecnologías; pero si se analizan de fondo estas prácticas podemos observar que el único cambio entre el Ingeniero Social del pasado y el Ingeniero Social de hoy es el medio que utiliza para llegar a sus víctimas, si se analiza a fondo estas estafas y deja establecida una base concisa sobre los métodos utilizados actualmente servirá para prevenir futuras prácticas.

Las causas principales de que una persona sea víctima es entre otras la desinformación y la indiferencia, si un usuario no tiene cuidado en proteger sus datos personales e información sensible, mucho menos le importara proteger datos de la empresa donde labora, información que puede causar grandes pérdidas a la empresa.

Otro aspecto a tomar en cuenta es que si una persona esta consistente de las amenazas en los sistemas de comunicación, implicaría una reducción en costos por mantenimiento en el caso de que la seguridad haya sido comprometida.

1.3.1- Importancia del estudio de Phishing.

El estudio presentado se enfoca particularmente en el método conocido como *Phishing*, esto es principalmente a que en la actualidad este es el método más usado por los ingenieros sociales, debido en gran parte a que su práctica es relativamente sencilla y eficaz, a diferencia de los métodos mencionados anteriormente.

Este método ha ido evolucionando con el uso de las nuevas tecnologías y se presentan casos diariamente en la actualidad, todos los días son recibidos correos electrónicos solicitando revisar datos personales en alguna red social o correos electrónicos donde bancos piden verificar la información de cliente, a veces también son recibidas invitaciones de mujeres atractivas para entablar amistad con ella, etc. Todos estos son ataques que por lo general usan para hacer *Phishing*.

De igual manera se presentan ataques no sólo en la computación, también se presenta en estafas con tarjetas de crédito, obtener información de una empresa, etc. Es por ello que es de gran importancia que la gente conozca un poco al respecto del tema ya que así se pueden evitar miles de fraudes que se comenten al año debido a esta práctica, de hecho el *Phishing* es un método tan importante en la Ingeniería Social que existen técnicas que se combinan con ella como es el caso de *Vishing* y *Spear Phishing*.

Ahora realizaremos un análisis de que es Phishing de una forma más profunda.

1.4-*Phishing*

Puede manifestarse en correos electrónicos engañosos y páginas web fraudulentas que aparentan proceder de instituciones de confianza como bancos o instituciones públicas, pero que en realidad están diseñados para conseguir información confidencial del usuario.

El *Phishing* funciona generalmente por medio de un correo electrónico, simulando proceder de una fuente fiable (por ejemplo, de una institución financiera), normalmente son mensajes que piden que el usuario cambie sus datos personales por razones de seguridad o de mantenimiento.

Después de acceder a la liga adjunta se es dirigido a una página similar a la del portal, permitiendo al estafador tener acceso a los datos que rellene el usuario. Para que el *Phishing* funcione se vale de técnicas de la Ingeniería Social.

Aunque el uso del correo electrónico es el medio que más utilizan los estafadores existen otros medios que también son explotados. El *Phishing* puede producirse de varias formas, desde un simple mensaje a su teléfono móvil, una llamada telefónica:

- *SMS (mensaje corto)*: Se recibe un mensaje donde se solicitan datos personales para poder recibir un premio o tiempo aire gratis.

- *Llamada telefónica*: Se pueden recibir llamadas telefónicas donde la persona que habla se identifica como trabajador de un organismo público o privado solicitando datos privados de la víctima.

- *Ventanas emergentes (Pop-up)*: Es una técnica muy clásica y bastante usada. En ella se pretende suplantar visualmente una imagen de un organismo oficial o empresas para que sean idénticas a las oficiales. También son utilizadas para promover publicidad engañosa para atraer a su víctima.

El *Pharming*. Consiste en manipular las direcciones del servidor de nombres de dominio o *DNS* por sus siglas en ingles. Cuando un usuario teclea una dirección en su navegador de internet, ésta debe ser convertida a una dirección *IP* numérica.
Este proceso es lo que se llama resolución de nombres, y de ello se encargan los servidores *DNS*. Sin embargo, utilizando ciertos tipos de *malware* que modifican el sistema de resolución de nombres local, ubicado en el archivo *HOSTS*, es capaz de redirigir a una página falsa incluso aun cuando el usuario haya tecleado la dirección en el navegador.
También se presenta la modalidad de lavado de dinero mediante el *Phishing*. Empresas ficticias reclutan trabajadores por medio de correos electrónicos, salones de *chat* y otros medios, ofreciendo trabajo desde casa. Para que una persona pueda iniciar a laborar en estas empresas se le pide que rellene un formulario donde, entre otros datos, se le pide su número de cuenta bancaria. Esto tiene la finalidad de ingresar en la cuenta del trabajador dinero procedente de estafas bancarias realizadas por otros métodos de *Phishing*.

Con cada acto fraudulento de *Phishing* la víctima recibe un ingreso en su cuenta bancaria y la empresa le notifica del hecho. Una vez recibido este ingreso, la víctima se quedará con un porcentaje como comisión de trabajo y el resto lo reenviará a través de sistemas de envío de dinero a cuentas indicadas por la supuesta empresa.

Dado el desconocimiento de la víctima (muchas veces motivado por la necesidad económica) ésta se ve involucrada en un acto de estafa importante, pudiendo ser requerido por la justicia previa denuncia de los bancos. Estas denuncias se suelen resolver con la imposición de devolver todo el dinero sustraído a la víctima, obviando que este únicamente recibió una comisión.

Otra modalidad es el conocido como *Spear Phishing*. 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. Podría parecer que el mensaje procede de un jefe o de un compañero que se dirige por correo electrónico a todo el personal (por ejemplo, el encargado de administrar los sistemas informáticos) y quizá incluya peticiones de nombres de usuario o contraseñas. En realidad, lo que ocurre es que la información del remitente del correo electrónico ha sido falsificada.

Mientras que las estafas de suplantación de identidad (*Phishing*) tradicionales están diseñadas para robar datos de personas, el objetivo de las de *Spear Phishing* consiste en obtener acceso al sistema informático de una empresa. Si responde con un nombre de usuario o una contraseña, o si hace clic en vínculos o abre datos adjuntos de un mensaje de correo electrónico, una ventana emergente o un sitio web desarrollado para una estafa de *Spear Phishing*, puede convertirse en víctima de un robo de datos de identidad y poner en peligro a su organización.

Las estafas de *Spear Phishing* también se dirigen a personas que utilizan un determinado producto o sitio web. Los timadores utilizan toda la información de que disponen para personalizar al máximo posible la estafa.

1.5- Delitos informáticos

Los avances tecnológicos especialmente los enfocados a la informática y las comunicaciones, en especial con la popularización de Internet, han cambiado, en muchos casos radicalmente, la forma de trabajar, compartir información y de pasar sus ratos libres. A principios de los años 80, incluso en los países más desarrollados, habría sido muy difícil imaginar muchas de las acciones cotidianas, como por ejemplo contar con una red de internet pública en parques y escuelas, navegar por Internet con un dispositivo móvil, etc.

De manera conjunta con estos avances en la tecnología, era obvio pensar, que estas tendrían consigo consecuencias no deseadas; en este caso, la proliferación de agentes que aprovechan los recursos del sistema y la buena intención o ignorancia del resto de actores para buscar ilícitamente el beneficio propio o del daño a terceros. De esta forma nacen los delitos informáticos o ciberdelitos.

Muchas de las personas que cometen los delitos informáticos poseen ciertas características específicas tales como la habilidad para el manejo de los sistemas informáticos o la realización de tareas laborales que le facilitan el acceso a información de carácter sensible. En algunos casos la motivación del delito informático no es económica sino que se relaciona con el deseo de ejercitar, y a veces hacer conocer a otras personas, los conocimientos o habilidades del delincuente en ese campo.
Muchos de los "delitos informáticos" encuadran dentro del concepto de "delitos de cuello blanco", término introducido por primera vez por el criminólogo estadounidense Edwin Sutherland en 1943[1]. Esta categoría requiere que: (1) el sujeto activo del delito sea una persona de cierto estatus socioeconómico; (2) su comisión no pueda explicarse por falta de medios económicos, carencia de recreación, poca educación, poca inteligencia, ni por inestabilidad emocional. El sujeto pasivo en el caso de los delitos informáticos puede ser individuos, instituciones crediticias, órganos estatales, etc. que utilicen sistemas automatizados de información, generalmente conectados a otros equipos o sistemas externos. Para la labor de prevención de estos delitos es importante el aporte de los damnificados que puede ayudar en la determinación del *modus operandi* esto es, de las maniobras usadas por los delincuentes informáticos.

[1] Sutherland, Edwin H. (1949). Delincuencia de cuello blanco de Nueva York. Holt Rinehart y Winston

1.5.1- El ciberdelito o delito informático.

Podemos definir al delito informático, crimen electrónico o ciberdelito, como aquel acto que agobia con operaciones ilícitas realizadas por medio de Internet y/o que tienen como objetivo destruir y dañar equipos, medios electrónicos y redes de Internet. Sin embargo, las categorías que definen un delito informático son aún mayores y complejas y pueden incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales equipos y redes han sido utilizados. Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados.

Existen actividades delictivas que se realizan por medio de estructuras electrónicas que van ligadas a un sin número de herramientas delictivas que buscan infringir y dañar todo lo que encuentren en el ámbito informático: ingreso ilegal a sistemas, interceptado ilegal de redes, interferencias, daños en la información (borrado, dañado, alteración), mal uso de artefactos, chantajes, fraude electrónico, ataques a sistemas, robo de bancos, ataques realizados por *hackers*, violación de los derechos de autor, pornografía infantil, pedofilia en Internet, violación de información confidencial y muchos otros.

A partir de las diferentes fuentes jurídicas pueden identificarse determinadas características de los delitos informáticos:

- *Transnacionalidad:* Los delitos informáticos trascienden las fronteras de los estados, lo que hace recomendable regulaciones también transnacionales de este tipo de actividades criminales.

- *Distancia física.* Los delincuentes nunca están en el "lugar del crimen" físicamente, por lo que su localización es más compleja y el riesgo que asumen es menor.

- *Complejidad derivada de la profesionalización y redes organizadas de ciberdelincuentes:* En numerosos casos las actividades fraudulentas son llevadas a cabo por mafias y redes de delincuentes organizadas y especializadas, frecuentemente ubicadas en otros países.

- *Ubicuidad*. Es posible cometer delitos de forma simultánea en lugares muy distantes.

De todas estas cuestiones, posiblemente la transnacionalidad es la más preocupante: un delincuente chino puede cometer una estafa en Estados Unidos estando físicamente en Italia a través de una red de computadoras (controlados remotamente) localizados en Rusia. Así pues, la complejidad procesal resultante de la coexistencia de diferentes tipos delictivos y la aplicabilidad de diversas legislaciones puede dificultar la persecución del delito. En base a las soluciones tradicionales, se suele abogar por la persecución del delito por parte de las autoridades del país en el que la víctima sufre sus consecuencias. Esta situación tiene una cierta utilidad práctica, que ha conducido a un relativo consenso en torno a su adopción.

1.5.2 Tipos de delitos informáticos.

Dado lo novedoso y la constante evolución de las formas delictivas a través de redes de comunicaciones, no existe una tipología universal de los delitos informáticos. Así, se plantean diferentes clasificaciones, según diversos criterios.

a) Crímenes que tienen como objetivo explotar debilidades dentro de redes de computadoras, por ejemplo, con la instalación de códigos, *gusanos* y archivos maliciosos, *spam*, ataque masivos a servidores de Internet y generación de virus.

b) Crímenes basados en técnicas de Ingeniería Social, son relativamente similares a los tradicionales "timos", en los que se engaña a la víctima para que haga algo (revelar información sensible de carácter personal e incluso cometer él mismo- de manera inconsciente- la actividad delictiva) que normalmente no haría y que va a ocasionar un perjuicio económico, ya sea a él o a terceros.

Otra clasificación interesante puede basarse en el objeto de los delitos informáticos. En este sentido, se pueden distinguir los delitos sobre las personas, los delitos sobre la propiedad privada y los delitos sobre las autoridades.

a) Respecto a los crímenes informáticos ejercidos sobre personas, en su mayoría son las versiones cibernéticas de algunas conductas tradicionalmente tipificadas como delictivas, por ejemplo, espionaje, fraude y robo, pornografía infantil, pedofilia, etc.

b) Los delitos informáticos sobre la propiedad se equiparan prácticamente a la mayor parte de formas de fraude tradicionales. Se incluyen dentro de este grupo todo tipo de violaciones de la propiedad, no sólo referidas al dinero (*Phishing*, *spam*, *cartas nigerianas*, *Pharming*, etc.), sino a la propiedad intelectual (*crackeo* o creación de *software* destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de computadora).

c) Finalmente, un tercer grupo de delitos informáticos puede tener como objetivo atacar a las autoridades de un país y, en definitiva, al sistema socio-económico de éste. Es el conocido como *ciberterrorismo*. El terrorismo virtual se ha convertido en uno de los novedosos delitos de los criminales informáticos los cuales deciden atacar masivamente el sistema computacional de una empresa, compañía, centro de estudios, oficinas oficiales, etc. Un ejemplo de ello lo ofrece un hacker de Nueva Zelandia, Owen Thor Walker (AKILL), quien en compañía de otros hackers, dirigió un ataque en contra del sistema de computadoras de la Universidad de Pennsylvania en 2006[2].

1.6- Regulación de los delitos informáticos en México

En México los delitos de revelación de secretos y acceso ilícito a sistemas y equipos de informática ya sea que estén protegidos por algún mecanismo de seguridad, se consideren propiedad del Estado o de las instituciones que integran el sistema financiero son hechos sancionables por el Código Penal Federal[3] en el titulo noveno capítulo I y II.

De acuerdo a la Constitución de los Estados Unidos Mexicanos, México es una república democrática, representativa y federal, compuesta de Estados libres y soberanos por lo que se refiere a su régimen interior, pero unidos en un pacto federal, en la siguiente podemos observar las legislaciones que contemplan delitos informáticos a nivel Federal.

[2] New Zealand Herald (2007). Bot-boy caught in his own net. http://www.nzherald.co.nz/file-sharing/news/article.cfm?c_id=199&objectid=10481058. Fecha de acceso diciembre 2011
[3] Código Penal Federal, publicado en el Diario Oficial de la Federación el 14 de agosto de 1931, última revisión publicada el 24/10/2011

1. Delitos Informáticos.
    - Código Penal Federal.
    - Ley Federal de Derechos de Autor.
    - Iniciativa de Ley Federal de Protección de Datos Personales.
2. Propiedad Intelectual.
    - Ley Federal de Derechos de Autor.
    - Ley de Propiedad Industrial.
3. Cómputo forense.
    - Código de Comercio.
    - Código Federal de Procedimientos Civiles.
4. Correo Electrónico.
    - Código Penal Federal.
5. Firmas y contratos digitales.
    - Código de Comercio.
    - Código Civil Federal.
    - Ley de Mercado de Valores.
6. Bases de Datos.
    - Ley Federal de Protección de Datos Personales.

Otras leyes relacionadas con los Delitos Informáticos:

- *Fraude mediante el uso de la computadora y la manipulación de la información que éstas contienen. (Técnica de salami u otras):* Artículo 231 del Código Penal para el D.F.[4] *"Se impondrán las penas previstas en el artículo anterior, a quien: ...* fracción XIV: *Para obtener algún beneficio para sí o para un tercero, por cualquier medio acceso, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la Institución...*

[4] Código Penal para el D.F., publicado en la Gaceta Oficial del Distrito Federal el 02 de febrero de 2007, última revisión publicada el 16/02/2011

- *Reproducción no autorizada de programas informáticos*: Regulada en la Ley Federal del Derecho de Autor[5], artículo 11 que establece el reconocimiento del Estado al creador de obras literarias o artísticas, entre las que están los programas de cómputo. *La reproducción queda protegida a favor del autor y se prohíbe la fabricación o uso de sistemas o productos destinados a eliminar la protección de los programas. El Código Penal Federal tipifica y sanciona esta conducta con 2 a 10 años de prisión y de 2000 a 20000 días de multa.*

- *Uso no autorizado de programas y de datos*: La Ley Federal del Derecho de Autor, en sus artículos 107 al 110, protege como compilaciones a las bases de datos legibles por medio de máquinas que por razones de disposición de su contenido constituyan obras intelectuales, otorgándole a su organizador el uso exclusivo por cinco años; asimismo, exceptuando las investigaciones de autoridades, la información privada de las personas contenida en bases de datos no podrá ser divulgada, transmitida ni reproducida salvo con el consentimiento de la persona de que se trate.

- *Intervención de correo electrónico*: El artículo 167 fracción VI del Código Penal Federal sanciona con uno a cinco años de prisión y 100 a 10000 días de multa al que dolosamente o con fines de lucro, interrumpa o interfiera comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transmitan señales de audio, de video o de datos. Aquí tipificaría el interceptar un correo antes de que llegue a su destinatario, pero no el abrir el buzón o los correos una vez recibidos.

- *Obtención de información que pasa por el medio*: Este tipo de conductas, que se refiere a interceptar datos que las personas envían a través de la red se tipifican en el artículo 167 fracción VI del Código Penal Federal a que hice referencia en el inciso anterior.

[5] Ley Federal de Derechos de Autor, publicada en el Diario Oficial de la federación el 24 de Diciembre de 2007, última revisión publicada el 23/07/2003

- *Acceso no autorizado a sistemas o servicios y destrucción de programas o datos.*

En la tabla 1.1 podemos observar las penas derivadas a las conductas ilícitas referentes a los sistemas de cómputo dentro de la República Mexicana.

Tabla 1.1 Sanciones tipificadas según el delito

CONDUCTA	PENA
▪ Destruir información sin autorización. ▪ Si se trata de sistemas o equipos del Estado. ▪ Si se trata de sistemas o equipos de las instituciones que integran el sistema financiero.	6 meses a 2 años prisión, 100 a 300 días multa 1 a 4 años y 200 a 600 días multa 6 meses a 4 años prisión, 100 a 600 días multa
▪ Conocer o copiar información sin autorización. ▪ Si se trata de sistemas o equipos del Estado. ▪ Si se trata de sistemas o equipos de las instituciones que integran el sistema financiero.	3 meses a 1 año prisión, 50 a 150 días multa 6 meses a 2 años prisión ,100 a 300 días multa 3 meses a 2 años prisión, 50 a 300 días multa
▪ Destruir información cuando se tenga autorización para el acceso. ▪ Si se trata de sistemas o equipos del Estado. ▪ Si se trata de sistemas o equipos de las instituciones que integran el sistema financiero.	2 a 8 años prisión y 300 a 900 días multa 6 meses a 4 años prisión y 100 a 600 días multa
▪ Conocer o copiar información cuando se tenga autorización para el acceso. ▪ Si se trata de sistemas o equipos del Estado. ▪ Si se trata de equipos de las instituciones que integran el sistema financiero.	1 a 4 años prisión y 150 a 450 días multa 3 meses a 2 años prisión y 50 a 300 días multa

1.6.1 Reglamentación del SPAM en México.

El *SPAM*, correo basura, mensajes basura de remitente desconocido, normalmente es aquel que llega a cuentas de correo sin haberlo pedido, por lo general las empresas que envían este tipo de correos consultan las listas públicas que circulan en Internet de manera "gratuita" y que obtienen su información con el simple hecho de que una persona haya enviado un mensaje personal. Este tipo de correo en México alcanzó de alguna manera su reglamentación el 19 de Mayo del 2003 y se hicieron adecuaciones el 4 de Febrero del 2004 en la Ley Federal de Protección al Consumidor[6]. Las reformas más importantes en materia publicitaria y de mercadotecnia se presentan en los artículos 17, 18 y 18 bis de la Ley Federal del Consumidor.

El Artículo 17 de dicha Ley nos dice: *En la publicidad que se envíe a los consumidores se deberá indicar el nombre, domicilio, teléfono y, en su defecto, la dirección electrónica del proveedor; de la empresa que, en su caso, envíe la publicidad a nombre del proveedor, y de la Procuraduría.*

Esto es, que para saber si se desea que nos llegaran ofertas de nuestros proveedores, se debe de haber dado datos confidenciales ya sea por medio de un enlace, por una conversación o por un correo electrónico.

La dirección del correo del Proveedor es importante, dado que en cualquier momento podemos pedir la baja de estos listados de envió de correo electrónico. Para esto último, se debe dar aviso, no solamente al proveedor, sino también a la Procuraduría Federal del Consumidor (PROFECO). Esto queda estipulado en el artículo 18 de la Ley Federal de Protección al Consumidor: *La Procuraduría podrá llevar, en su caso, un registro público de consumidores que no deseen que su información sea utilizada para fines mercadotécnicos o publicitarios. Los consumidores podrán comunicar por escrito o por correo electrónico a la Procuraduría su solicitud de inscripción en dicho registro, el cual será gratuito.*

[6] Ley Federal de Protección al Consumidor, publicado en el Diario Oficial de la Federación el 24 de diciembre de 1992, última revisión 26/05/2011

El artículo 18 BIS de la Ley Federal de Protección al Consumidor dice: *Queda prohibido a los proveedores y a las empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios y a sus clientes, utilizar la información relativa a los consumidores con fines diferentes a los mercadotécnicos o publicitarios, así como enviar publicidad a los consumidores que expresamente le hubieran manifestado su voluntad de no recibirla*.

Si aun así, después de haber decidido dar de baja de las bases de los proveedores y dar aviso a la PROFECO de no querer recibir mensajes electrónicos no deseados, siguen las prácticas se puede actuar jurídicamente para que el proveedor se haga acreedor a alguna multa estipulada dentro del artículo 127 de la Ley Federal de Protección al Consumidor: *Las infracciones a lo dispuesto por los artículos…. 17, 18 BIS… serán sancionadas con multa de $397.76 a $1'272,813.16*.

1.6.2 La policía cibernética en México.

El manejo y el uso de la información en la red de redes, tiene muchas aristas por explorar. Existen vacíos en los sistemas de seguridad informática, así como en la aplicación y formulación de leyes; dicha situación convierte a Internet en un espacio propicio para la ejecución de delitos cibernéticos. Según una iniciativa de ley propuesta el 22 de marzo de 2000 ante el pleno de la Cámara de Senadores de la Quincuagésima Legislatura, están consideradas como delitos informáticos "todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen referencia al uso indebido de cualquier medio informático."El robo o alteración de información, sabotaje, pedofilia, tráfico de menores, fraude, clonación de señales satelitales, de tarjetas de crédito y el ciberterrorismo son actividades consideradas por las autoridades de los tres niveles (federal, estatal y municipal) como una muestra de estos ilícitos, los cuales día con día muestran un incremento en México, expandiéndose de manera considerablemente rápida.

Uno de los problemas más importantes para la persecución de estos delitos tiene que ver con la rapidez que ofrece la publicación electrónica para poner y quitar información de cualquier tipo y formato Web.

Para contrarrestar éstos y otros delitos cibernéticos de creciente expansión, el gobierno mexicano conformó un equipo especializado llamado DC México (Delitos Cibernéticos México), este grupo lo integran todas las corporaciones policiacas estatales y federales, así como los proveedores de servicio de Internet, (ISPs) y todas las compañías privadas o públicas que ofrecen seguridad informática en el país. DC México tiene como tareas fundamentales la identificación, el monitoreo y el rastreo de cualquier manifestación delictiva que se cometa mediante computadoras conectadas en territorio mexicano o fuera de él y que tenga afectaciones en nuestro país.

La Universidad Nacional Autónoma de México participa en este grupo con UNAM-CERT, que es un organismo importante por las contribuciones que ha realizado en materia de prevención del delito. El UNAM-CERT se encarga de proveer el servicio de respuesta a incidentes de seguridad en cómputo a sitios que han sido víctimas de algún "ataque", así como de publicar información respecto a vulnerabilidades de seguridad, alertas de la misma índole y realizar investigaciones de la amplia área del cómputo y así ayudar a mejorar la seguridad de los sitios.

1.6.3 El Instituto Federal de Acceso a la Información y Protección de Datos (IFAI).

El Instituto Federal de Acceso a la Información Pública y Protección de Datos (IFAI) es un organismo Mexicano descentralizado de la Administración Pública Federal, no sectorizado y que goza de autonomía operativa, presupuestaria y de decisión, encargado de garantizar el derecho a él acceso a la información pública gubernamental, brindar protección de datos personales que están en manos del gobierno federal y resolver conflictos sobre negativas referentes al acceso a información que las dependencias, entidades del gobierno federal o particulares hayan formulado.

El IFAI nace como disposición de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, aprobada y puesta en vigor el 12 de junio de 2003. A partir de esta ley, en 2007, se reforma el artículo 6° de la Constitución Política de los Estados Unidos Mexicanos garantizando como derecho fundamental el acceso a la información.

En 2010, el Congreso de la Unión aprobó la Ley Federal de Protección de Datos Personales en Posesión de Particulares, lo cual amplió las facultades y responsabilidades del IFAI cambiando su nombre al de "Instituto Federal de Acceso a la Información y Protección de Datos". A partir de julio del mismo año, el IFAI inició un proceso de reestructuración y capacitación tanto de su personal como de todos aquellos sujetos, físicos o morales, poseedores de una base de datos, el cual concluirá en enero de 2012, fecha en la que el derecho de las personas a ser protegidas en sus datos tendrá plena vigencia. Los principales objetivos del IFAI son:

a) Facilitar y garantizar el acceso de las personas a la información pública y el acceso y protección que obren en las dependencias y entidades de la Administración Pública Federal, así como contribuir con la organización de los archivos nacionales.

b) Promover la cultura de la transparencia en la gestión pública y en la rendición de cuentas del gobierno a la sociedad, así como el ejercicio de los derechos de los gobernados en materia de acceso a la información y protección de datos personales.

c) Contribuir en el proceso de análisis, deliberación, diseño y expedición de normas jurídicas necesarias en materia de archivos y de datos personales, así como los procedimientos legislativos dirigidos a perfeccionar y consolidar el marco normativo y constitucional en materia de transparencia y acceso a la información pública.

Las acciones que se pueden realizar a través del IFAI es la solicitud de información, enviar una queja por falta de respuesta a una solicitud y el recurso de revisión.

Una solicitud es un trámite mediante el cual las personas pueden acceder a la documentación que generan, obtienen o conservan las dependencias o entidades de la administración pública y otros sujetos obligados como los poderes legislativo y judicial, organismos constitucionales autónomos y tribunales administrativos federales.

En caso de una queja por falta de respuesta el IFAI verificara que la entidad o dependencia no dio ninguna notificación, si continúa la falta de respuesta en un plazo de 20 días hábiles, el IFAI obligara a la dependencia a dar acceso a la información y si es necesario, también obligara a pagar los costos de reproducción del material. El recurso de revisión es un trámite mediante el cual las personas pueden inconformarse cuando no está de acuerdo con la respuesta de una institución a una solicitud de información como en el caso de recibir información incompleta o errónea o nos niega el acceso a la modificación de datos personales.

Para poder realizar estos trámites el IFAI pone a disposición el servicio de INFOMEX a través de su página www.infomex.org.mx o si no se cuenta con servicio de Internet se puede elaborar un escrito y llevarlo directamente al IFAI o a la unidad de enlace de la entidad correspondiente.

1.6.4 Ley Federal de Transparencia y Acceso a la Información Pública.

Esta ley nace en el 2002 con el propósito de cumplir dos demandas: la primera se refiere a cumplir la demanda democrática de un gobierno totalmente público sin que este se reserve privilegios de cualquier tipo. La segunda es cumplir la demanda civil de un estado capaz de garantizar la seguridad de datos personales. La Ley Federal de Transparencia y Acceso a la Información pública Gubernamental[7] ofrece vías rápidas y claras para ejercer el derecho al acceso de información sin restricción de tipo.
Esta ley contiene 64 artículos divididos en 3 títulos, el primer título compete a la investigación presentada.

- El primer capítulo nos habla acerca de las disposiciones generales, la definición de esta ley como pública y obligatoria para funcionarios públicos y los objetivos de esta ley como: prever lo necesario para que toda persona pueda tener acceso a la información, transparentar la gestión pública mediante la difusión de la información, garantizar la protección de los datos personales, favorecer la rendición de cuentas a los ciudadanos, mejorar la organización, clasificación y manejo de los documentos.

[7] Ley Federal de Transparencia y Acceso a la Información pública Gubernamental publicada en el Diario Oficial de la Federación el 11 de junio del 2002, última revisión publicada el 05/07/2010

- El segundo capítulo trata acerca de las obligaciones de la transparencia, los artículos contenidos en esta sección se refieren a la exposición obligatoria de información y actualización por parte de los organismos mencionados en esta ley.

- El tercer capítulo menciona las excepciones en la cual se puede reservar el derecho a brindar información como es el caso de comprometer la seguridad nacional, la seguridad pública o la defensa nacional, deteriorar las relaciones internacionales, incluida aquella información con carácter de confidencial al Estado Mexicano, dañar la estabilidad financiera del país, poner en riesgo la vida, la seguridad o la salud de cualquier persona y causar un serio perjuicio en la impartición de la justicia. También nos menciona acerca de la información que puede darse bajo reserva protegiendo información confidencial como información gubernamental confidencial, secretos comercial, industrial, fiscal, bancario o averiguaciones previas.

- El cuarto capítulo nos habla acerca de la protección de datos personales en el cual se menciona las obligaciones que se deben cumplir para garantizar la seguridad de los datos personales, tratar datos personales sólo cuando éstos sean adecuados, poner a disposición de los individuos el documento en el que se establezcan los propósitos para su tratamiento, procurar que los datos personales sean exactos y actualizados. Además nos habla de las responsabilidades en el manejo de datos personales como adoptar los procedimientos para recibir y responder las solicitudes de acceso y corrección de datos, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos, tratar datos personales sólo cuando éstos sean adecuados, poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales y procurar que los datos personales sean exactos y actualizados.

- El último capítulo de la primer título nos habla acerca de los costos para obtener información el cual no debe ser mayor al material utilizado para su reproducción y el gasto de envió.

1.6.5 Lineamientos de Protección de Datos Personales.

Considerando el derecho a la vida privada plasmado en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos el cual menciona que "nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento".

Pero con el avance vertiginoso de la tecnología, las personas han adquirido una series de ventajas que contribuyen a mejorar su calidad de vida y, en el caso del Estado, a mejorar la actividad administrativa, el desarrollo económico, social y cultural, así como el cumplimiento de las obligaciones ciudadanas, pero al mismo tiempo, haciendo una mala utilización de las herramientas tecnológicas puede convertirse en un factor de amenaza a la privacidad y seguridad de las personas ya que las nuevas tecnologías permiten él movimiento de grandes volúmenes de información. Para atender este problema surge la Ley Federal de Transparencia y Acceso a la Información Pública en su apartado de Protección de Datos Personales. Las últimas reformas a Los Lineamientos de Protección de Datos Personales aparecieron publicadas en el diario oficial de la federación el 30 de septiembre del 2010 está dividida en 8 capítulos:

- El primer capítulo se compone de disposiciones generales, los objetivos generales y procedimientos que deberán observar las dependencias y entidades de la Administración Pública Federal para garantizar el adecuado tratamiento de datos personales.

- El segundo capítulo trata de los principios de protección de datos personales el cual los organismos deberán observar los principios de licitud, calidad, acceso y corrección, de información, seguridad, custodia y consentimiento para su transmisión.

- El tercer capítulo trata de cómo debe ser el tratamiento de datos personales los cuales deben ser:
-
    - Exactos, es decir que los datos personales se mantienen actualizados.

- Adecuados: Cuando se observan las medidas de seguridad aplicables.
- Pertinente: Cuando es realizado por el personal autorizado para el cumplimiento de las atribuciones de las dependencias y entidades que los hayan recabado, y
- No excesivo: Cuando la información solicitada al Titular de los datos es estrictamente la necesaria para cumplir con los fines para los cuales se hubieran recabado.

- El cuarto capítulo habla de la forma en que pueden ser transmitidos los datos personales y los requisitos para que el titular de los datos pueda ceder su transmisión.

- El quinto capítulo habla de las medidas de seguridad que deben adoptar los titulares de las dependencias y entidades, las forma en que se deben almacenar los datos personales, la seguridad en la red, el control de acceso y las recomendaciones sobre los estándares mínimos de seguridad.

- El sexto capítulo habla acerca de cómo debe ser el registro de datos personales dentro del sistema "Persona" el cual está diseñado por el IFAI y permite el almacenamiento y búsqueda de datos personales cumpliendo así los lineamientos establecidos en la ley de Transparencia.

- El séptimo y último capítulo nos hablan acerca de las acciones que pueden tomar las instituciones en caso de presentarse irregularidades de parte de un servidor público.

1.6.6 Ley de protección de datos personales para el Distrito Federal.

En 2008 se legisló por primera vez en el Distrito Federal sobre la materia de la protección de los datos personales. Esta ley surgió de la obligación que tiene el estado de proteger la información de carácter personal y asegurar sus derechos su derecho a la privacidad. El derecho a la protección de datos consiste en un poder de disposición y de control sobre los datos personales, los cuales se concretan en la facultad de consentir la recolección, obtención y acceso a los datos para su posterior almacenamiento y tratamiento, así como su uso o usos posibles por un tercero, en este caso por el estado o un particular que, con motivo de una relación contractual con las autoridades públicas del Distrito Federal, requiera tratar los datos.

Esta obra permite identificar claramente las distinciones existentes entre el derecho de acceso a la información, el cual es regulado en la Ley de Transparencia y Acceso a la Información pública del Distrito Federal[8], y el derecho a la protección de los datos personales, que es un derecho plenamente autónomo al derecho de acceso a la información, como lo comprueba su reciente inclusión en el artículo 16 de la Constitución Política Federal.

La ley de protección de datos personales está dividida en cinco títulos:

La primera parte se enfoca en las disposiciones comunes para los entes públicos en la cual define que esta ley es de orden público e interés general y que tiene como objetivo establecer los principios, derechos, obligaciones y procedimientos que regulan la protección de datos personales.

El segundo título habla de la tutela de datos personales dividido en 5 capítulos, el primer capítulo trata de los principios que deben tener un sistema de datos entre ellos destacan que los datos se regirán por los principios de licitud, consentimiento, calidad en los datos, confidenciales, seguros, disponibles y temporales.

El segundo capítulo nos habla cómo los organismos deben manejar la creación, modificación o supresión de datos personales así como deben de ser publicada y justificadas estas acciones. También nos dice cómo los organismos se ven obligados a informar a los interesados acerca de la inclusión de sus datos personales y finalmente nos dice que ninguna persona puede ser obligada a proporcionar datos de carácter racial, moral, de ideología, preferencias sexuales o religión.

El tercer capítulo nos habla de las medidas de seguridad que ofrecen los entes públicos para garantizar la confidencialidad e integridad del sistema de datos, nos habla además de que los entes federales deberán establecer diferentes tipos de seguridad a nivel físico, lógico, de las aplicaciones, de cifrado o de redes así como establecer niveles de seguridad.

[8] Ley de Transparencia y Acceso a la Información pública del Distrito Federal publicada en la Gaceta Oficial del Distrito Federal el 28 de Marzo del 2008 sin nuevas revisiones hasta la fecha

El cuarto capítulo nos menciona como deben ser tratados los datos personales, en él nos habla que el interesado deberá cumplir una serie de requisitos para la consulta de datos y garantizar que estos datos no sean usados para malas prácticas.

El último capítulo del segundo título trata de las obligaciones de los entes públicos en el manejo de los datos personales, entre las observaciones destacan que los entes públicos deberán cumplir con las políticas en el manejo, seguridad y protección de datos, no hacer mal uso de la información y solo utilizarla si realmente es requerida, y elaborar planes de capacitación en materia de seguridad.

El tercer título contiene un capitulo único y nos habla acerca de las capacidades y atribuciones que tiene el instituto de acceso a seguridad pública del distrito federal que entre otras funciones, es el encargado en cumplir la ley aquí comentada así como las normas que deriven. Algunas de las atribuciones más importantes que tiene el instituto son: establecer políticas y lineamientos para el manejo, tratamiento, seguridad y protección de datos personales, así como expedir nuevas normas que sean necesarias para el cumplimiento de esta ley, diseña y aprueba formatos de solicitud de acceso o modificación de datos personales y elaborar y publicar estudios e investigaciones para difundir el conocimiento de esta ley.

El cuarto título habla acerca de los derechos y el procedimiento para su ejercicio, dividido en tres capítulos, el primero de estos nos habla de los derechos en materia de datos personales, este apartado nos dice que cualquier persona debidamente identificada, contará con los derechos de acceso, rectificación, cancelación y oposición de sus datos personales. El segundo capítulo nos habla de cómo debe ser el procedimiento para ejercer el derecho mencionado en el capítulo pasado.

El último capítulo de este apartado nos menciona el derecho al recurso de revisión en caso de que el interesado se considere agraviado al haber requerido una solicitud de acceso, rectificación, cancelación u oposición o la omisión de una respuesta.

Finalmente el último título nos habla de las infracciones a la presente ley como lo pueden ser:

- la omisión o irregularidad en las solicitudes de acceso.
- impedir o negar el ejercicio de los derechos que se refiere la presente ley.
- recabar datos sin proporcionar la información prevista en la ley.
- obtener datos personales de manera engañosa o fraudulenta.
- alterar, destruir o transmitir datos fuera de los casos permitidos.

CAPÍTULO II

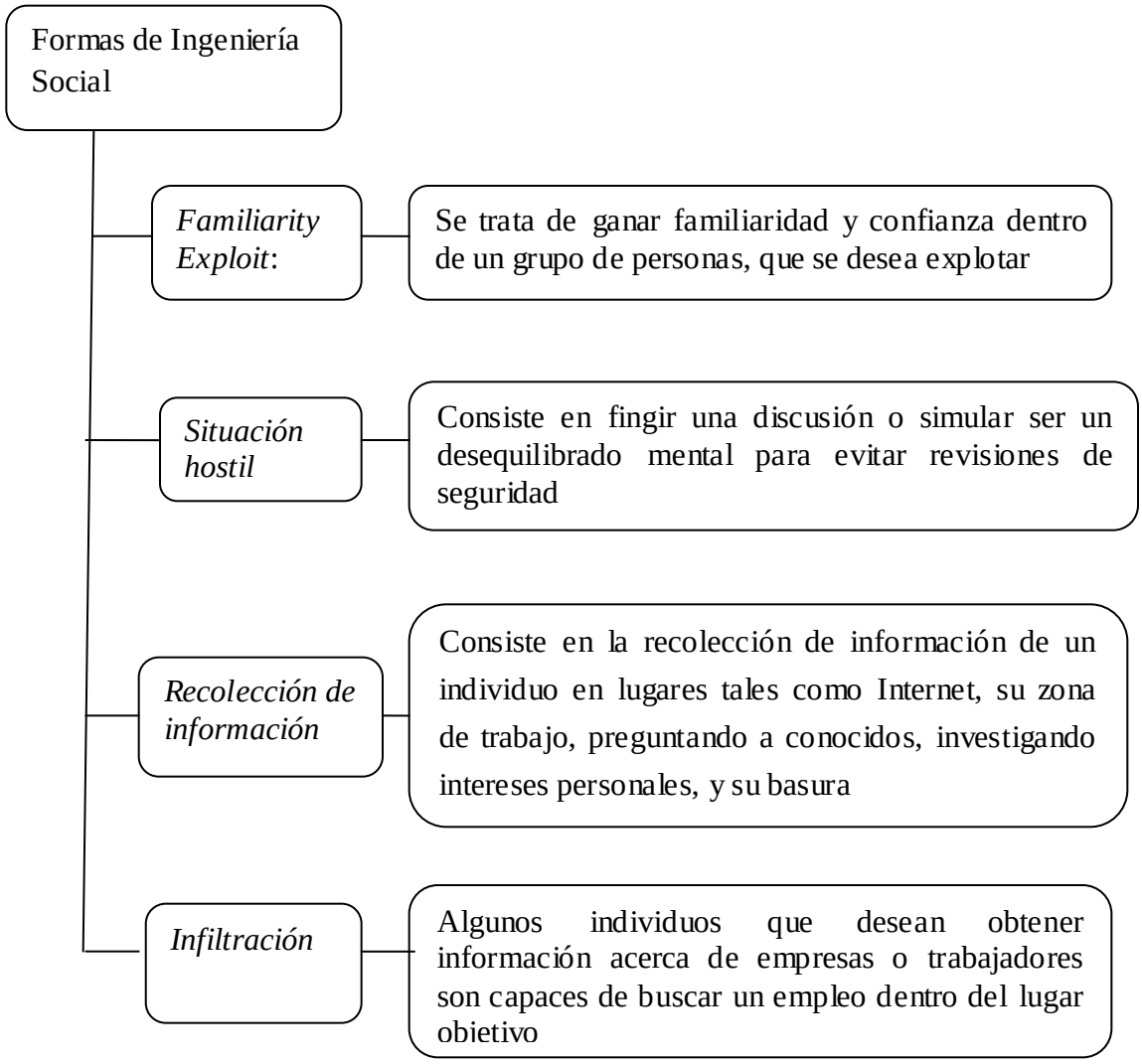
TÉCNICAS DE LA INGENIERÍA SOCIAL

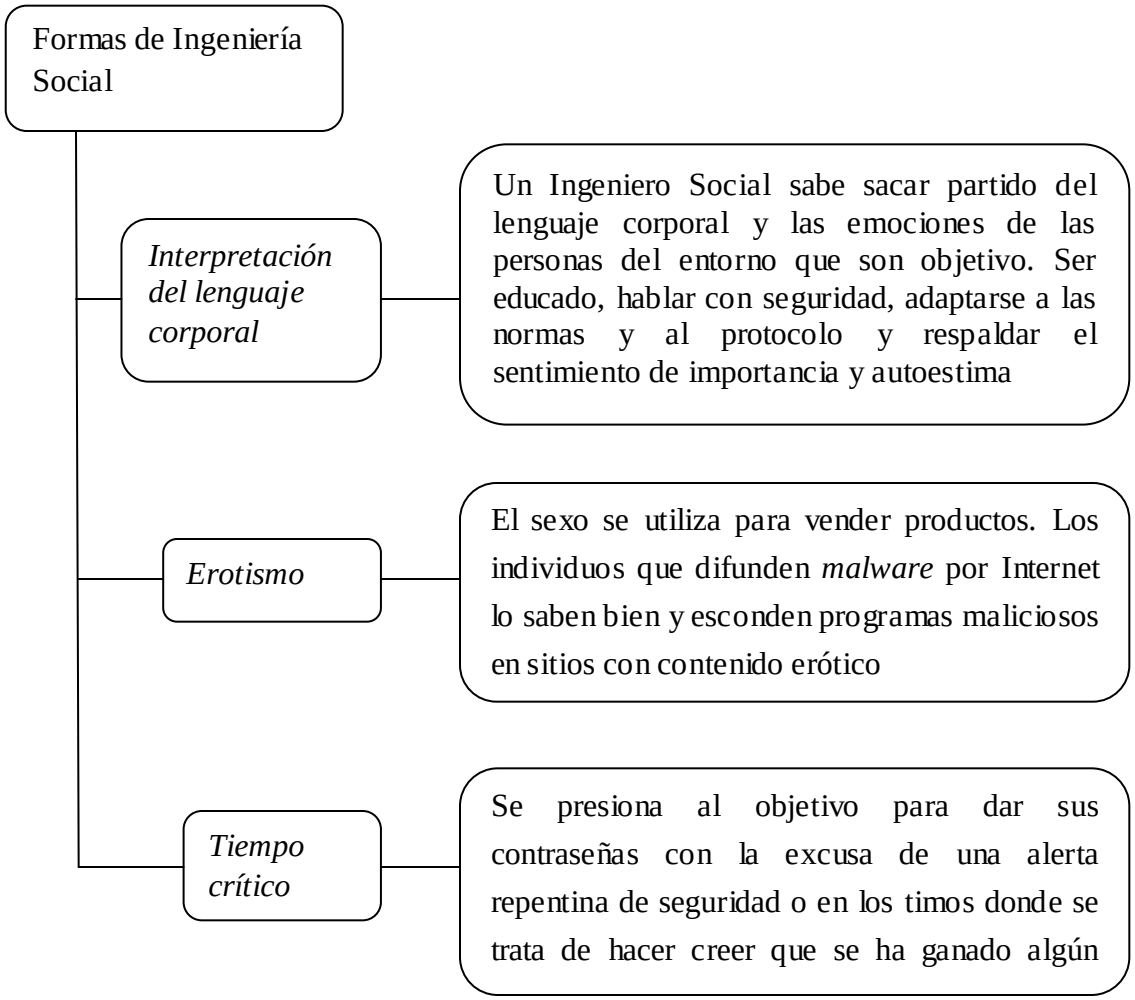
Se revisarán las principales técnicas que se usan los Ingenieros Sociales para atacar a los usuarios.

CAPÍTULO II TÉCNICAS DE LA INGENIERÍA SOCIAL

2.1- Técnicas de Ingeniería Social

A continuación se presentaran algunas de las técnicas más comunes utilizadas por el Ingeniero Social, aunque un ataque verdadero puede presentar combinación de dos o más de estas técnicas.

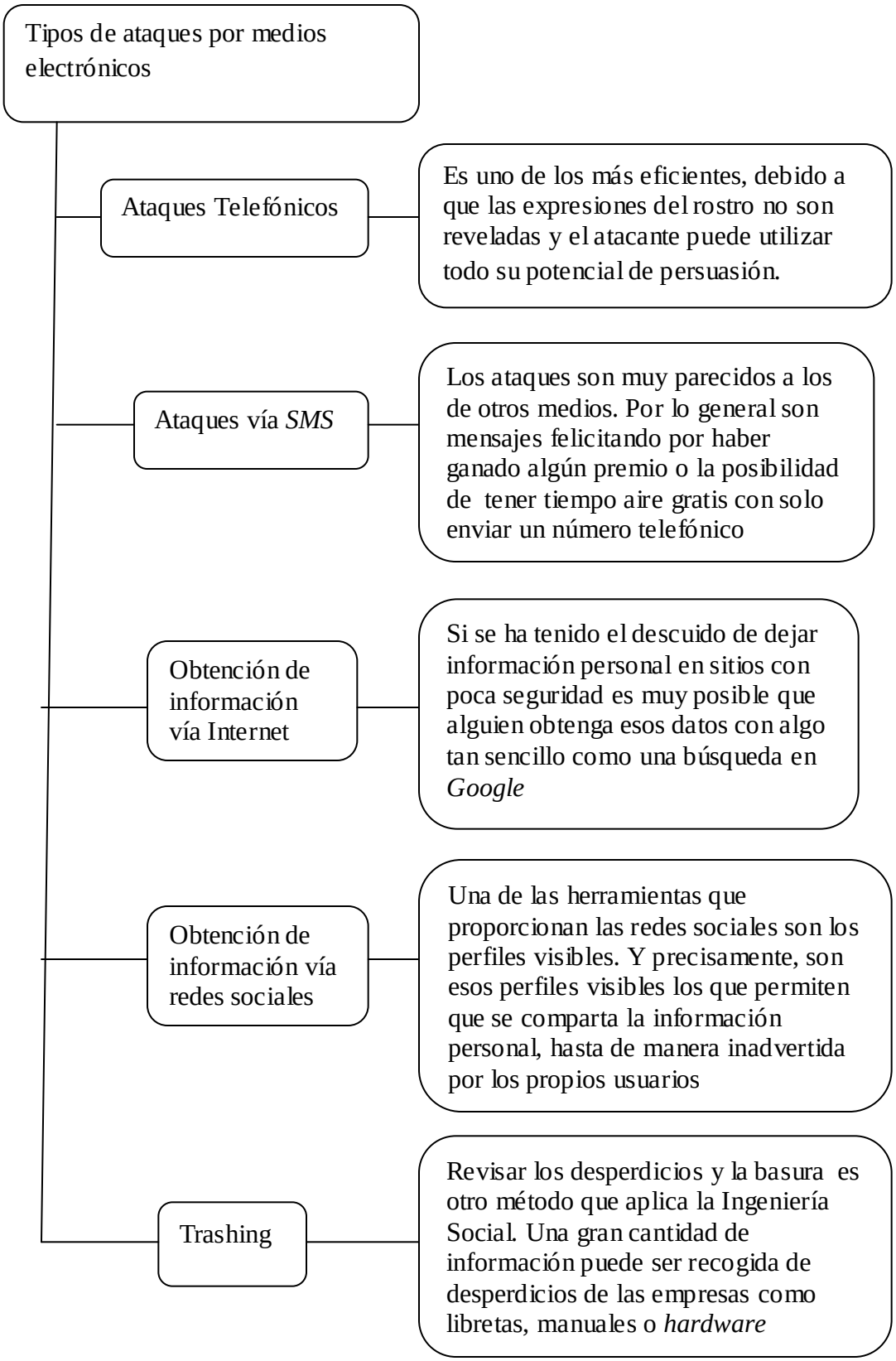




2.2-Tipos de ataques por medios electrónicos

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

Aunque las formas dichas con anterioridad son las más utilizadas, han ido evolucionando a una nueva forma de ataques utilizados las nuevas tecnologías como virus para dispositivos móviles o portales engañosos que asemejan un sitio genuino.


Tipos de ataques por medios electrónicos
Ataques Telefónicos
Es uno de los más eficientes, debido a que las expresiones del rostro no son reveladas y el atacante puede utilizar todo su potencial de persuasión.
Ataques vía *SMS*
Los ataques son muy parecidos a los de otros medios. Por lo general son mensajes felicitando por haber ganado algún premio o la posibilidad de tener tiempo aire gratis con solo enviar un número telefónico
Obtención de información vía Internet
Si se ha tenido el descuido de dejar información personal en sitios con poca seguridad es muy posible que alguien obtenga esos datos con algo tan sencillo como una búsqueda en *Google*
Obtención de información vía redes sociales
Una de las herramientas que proporcionan las redes sociales son los perfiles visibles. Y precisamente, son esos perfiles visibles los que permiten que se comparta la información personal, hasta de manera inadvertida por los propios usuarios
Trashing
Revisar los desperdicios y la basura es otro método que aplica la Ingeniería Social. Una gran cantidad de información puede ser recogida de desperdicios de las empresas como libretas, manuales o *hardware*

Otra variante de ataque es el conocido como *Malware*: El *Malware* (termino formado a partir de combinar las palabras *Software* Malicioso) es un programa diseñado para hacer algún daño a un sistema. Puede presentarse en forma de virus, *gusanos, caballos de troya, etc*., este *malware* generalmente es camuflajeado para parecer un archivo inofensivo o incluso ejecutarse en segundo plano mientras corre alguna otra aplicación. De los *malware* más comúnmente difundidos son los *virus y gusanos* por su capacidad de auto replicarse e infectar redes completas.

- *Virus*. Es un *malware* que necesita un portador para ser propagado como lo son archivos ejecutables que incorporan las aplicaciones, las memorias USB, y los archivos que contengan macros.

- *Troyano*. Es un programa dañino, que suele presentarse disfrazado de otro programa o como pequeña parte de un archivo que parece indefenso, no tienen la capacidad de auto-replicarse, pero pueden ser adheridos a cualquier tipo de software. Por ejemplo, un archivo adjunto recibido en un mail que al abrir un archivo de imagen efectivamente muestra la imagen pero a su vez se ejecuta un programa que el usuario no conoce.

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

- *Keylogger*. Es un programa malicioso que registra cada vez que se pulsa una tecla y se almacenan en un archivo de texto. Estos programas están pensados para robar información privada de una persona, como por ejemplo números de identificación personal. Las principales víctimas de los *keylogger* son personas que utilizan el servicio de cibercafés, debido a que estos poseen un escaso mecanismo de seguridad o en el peor de los casos, son los dueños los que buscan obtener información de sus clientes.

- *Exploit*. Es un programa que aprovecha alguna debilidad de un sistema operativo. Los *Exploit* no necesariamente son maliciosos. Generalmente los crean expertos para demostrar que existe un fallo en la seguridad del sistema.

- G*usanos.* A diferencia de los virus, no dependen de un archivo portador para funcionar es decir requiere que un usuario lo instale.

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

➢ *Spam*: El Spam se considera como el envío masivo y no solicitado de correo electrónico, normalmente con contenido publicitario de productos o servicios dudosos. Este tipo de correo puede pasar de solo una molestia a ser verdaderamente perjudiciales ya que pueden contener algún tipo de *malware* escondido.

  Las características más comunes del Spam son:

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

Si bien se conoce al *Spam* por medio del correo electrónico, no es su única ruta de distribución. Este fue evolucionando, desde los correos electrónicos, pasando por los programas de mensajería instantánea hasta los celulares y las conversaciones telefónicas por *VoIP*.

Cada cual tiene su nombre y estos son:

- *Spam*: enviado a través del correo electrónico.
- *Spim*: *Spam* sobre mensajería instantánea (*MSN Messenger*, etc.).
- *Spam SMS*: Spam que se difunde por dispositivos celulares mediante la tecnología *SMS*.
- *Spit*: *Spam* sobre telefonía IP también conocida como *VoIP*.

2.3- Herramientas de *Phishing*

Existen varias formas de realizar *Phishing* las herramientas que se mencionarán a continuación son las más comunes y las más usadas en la ingeniería social para el robo de información.

2.3.1- Kits de herramientas de Phishing.

En el internet existen *kits* de creación de *Phishing* estos son:

- *Alojar una página clonada de algún dominio.* Ésta se basa en páginas *HTML*, *JavaScript*, etc. Para ello es necesario suplantar una página concurrida para que la gente la visite, para ello obtendremos información de los usuarios que pretendan iniciar sesión para usar determinadas páginas algunos ejemplos son: páginas de bancos, redes sociales, páginas de servicios de alojamiento, etc.

  Podemos citar como ejemplo: Al iniciar sesión a los servicios de MSN se recibe un correo electrónico el cual pide que se verifique los datos de usuario pero como se observa en la *Figura 2.1*, el enlace incluido en el correo dirige a una página de apariencia similar al portal de MSN pero con un dirección diferente.

Figura 2.1 Portal falso de Hotmail

- *Lógica del robo de contraseñas*. Es un programa *PHP* que envía las contraseñas de formularios por correo electrónico, también puede almacenarlas en un archivo en el propio servidor, el atacante las obtendrá de ahí más adelante. Suelen ser apenas unas líneas de código muy sencillas. La mayoría de estos pueden encontrarse en el internet o en diversos *kits* que se encuentran fácilmente, estos dejan todo preparado para que el usuario solo deba modificar la dirección a la que quiere que vayan a parar las contraseñas robadas.

  Dos de los ejemplos más recientes son las páginas "quien te admite y no admitido" destinadas a robar el nombre y contraseña de los usuarios de MSN a cambio de mostrarles a los visitantes que las utilicen, quien los ha borrado de su lista de contactos. Como se muestra en la *Figura 2.2*, se observa un anuncio que invita la instalación de este programa.

  El servicio que brindan puede obtenerse fácilmente desde la solapa "privacidad" del menú opciones desde el MSN. Sin embargo, como muchos usuarios desconocen esta opción, son estafados.

Figura 2.2 Ejemplo de intento de Phishing, con mensaje falso del servicio de mensajería instantánea

- *Correo electrónico***.** Suele contener un logotipo y ser enviado de forma masiva a miles de cuentas de correo. Se suelen utilizar programas específicos para el envío masivo de correos o programas, también en *PHP* que se aprovechan del correo de páginas de terceros. Por ejemplo enviando *spam* a los contactos del correo obtenido, así como también invitarlos a usar algún servicio de forma gratuita, etc.

  Un ejemplo claro es el mostrado en la *Figura 2.3*, en este caso se han valido de la imagen de *PayPal* para intentar hacer un robo de cuentas bancarias. En un correo electrónico recibimos una liga, que de no ser la extraña dirección de correo podríamos llegar a creer que es de *PayPal* genuinamente.

  En el correo electrónico se argumenta que debido a un incumplimiento de facturación se necesitan los datos para desbloquear la cuenta. Para poder seguir con el procedimiento se pide que se acceda a una dirección que parece de *PayPal* y que se notificará con otro correo en el momento que la cuenta esta reactivada. El correo acaba con todos los datos de *PayPal* y por supuesto está encabezado con el logo de la compañía.

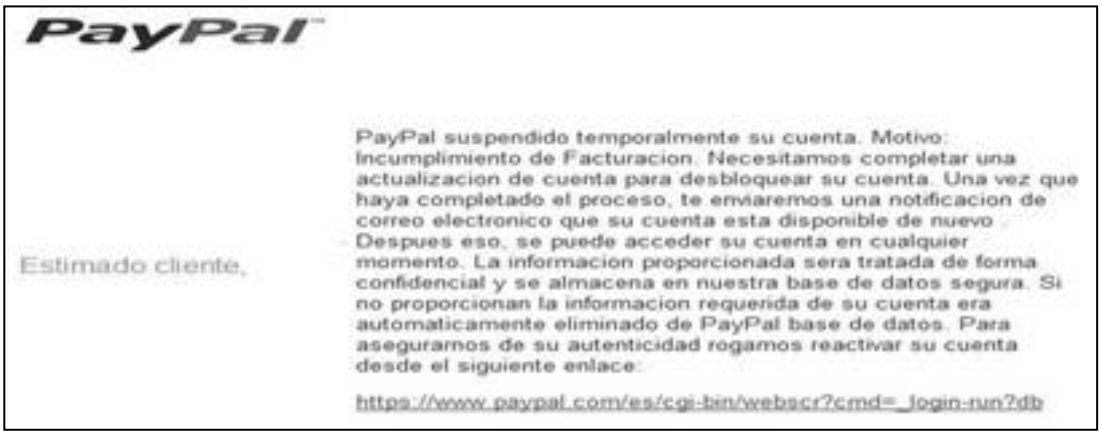


Figura 2.3 Correo electrónico suplantando (PayPal)

2.3.2- Herramientas de elaboración de páginas.

Algunas herramientas para obtener la información del usuario son relativamente simples solo es necesario descargar algún programa de la *web*, algunos ejemplos son: *Frontpage, Dreamweaver, SET, Metasploit, etc*. Y usar con ello un poco de malicia y la ingenuidad de los usuarios.

- *Frontpage.- Microsoft FrontPage* es un editor de páginas web para el operativo *Windows*. Formó parte de la suite *Microsoft Office*. Muchos consideran que el código *HTML* generado por esta aplicación es un poco descuidado y muchas veces reiterativo, especialmente en versiones antiguas.
- *Dreamweaver.- Adobe Dreamweaver* es la aplicación que lidera el sector de la edición y creación de contenidos *web*. Proporciona funciones visuales y de nivel de código para crear diseños y sitios web basados en estándares para equipos de sobremesa, teléfonos inteligentes, tabletas y otros dispositivos.

2.3.3 Kit de herramientas del Ingeniero Social (SET).

Es una suite desarrollada en *Python* que consta de herramientas específicamente diseñadas para realizar ataques al elemento humano usando como método la Ingeniería Social en procesos de auditoría en seguridad (pruebas de penetración).Está programado por David Kennedy (ReL1K).

Instalación

SET es multiplataforma, así que sólo necesitaremos tener instalado el intérprete de *Python* -en caso de usar *Windows*- para poder ejecutarlo. Para descargar *SET* debemos de ejecutar en la terminal lo siguiente:

windhack@laptop ~ $ svn co http://svn.secmaniac.com/social_engineering_toolkit set/

Posteriormente ejecutamos como root:

```
windhack@laptop ~/set $ sudo ./set
[sudo] password for windhack:
Error!!! BeautifulSoup is required in order to fully run SET
Please download and install BeautifulSoup:
http://www.crummy.com/software/BeautifulSoup/download/3.x/BeautifulSoup
-3.0.8.1.tar.gz
Would you like SET to attempt to install it for you?
yes or no: yes
```

Automáticamente nos da la opción de descargar e instalar por medio de la misma herramienta. Luego volvemos a ejecutar como se muestra en la *Figura 2.4*

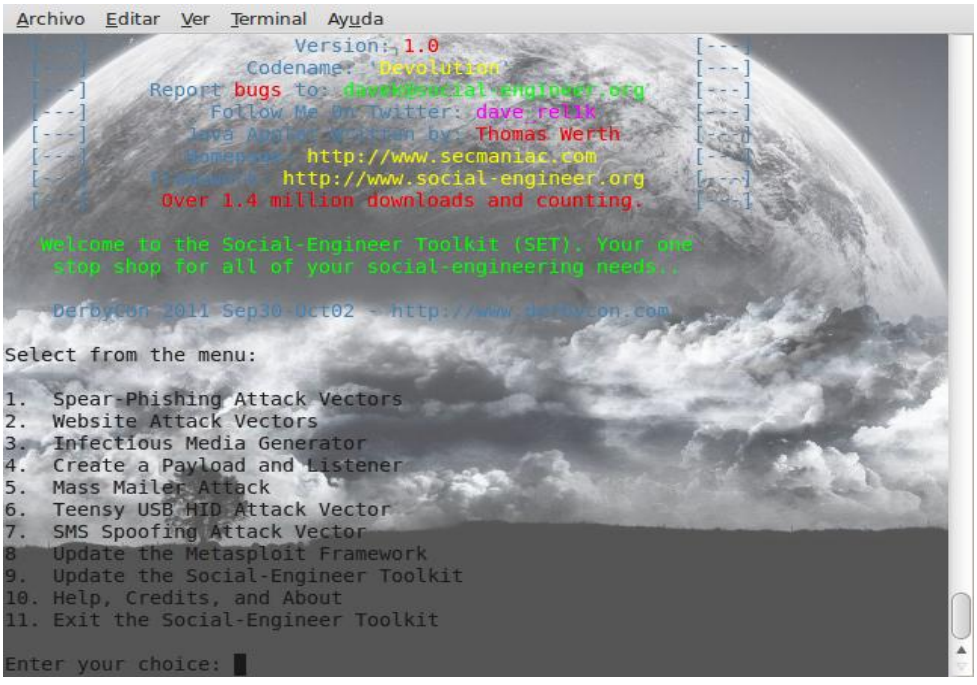


Figura 2.4 Instalación de Social-Engineer Toolkit (SET)

A continuación veremos algunas de las principales opciones del *SET*.

- *Sistema de Phishing*. Este sistema es bastante completo como se muestra en la *Figura 2.5*. Permite la creación automática de un sitio web falso para engañar al destinatario. También se pueden enviar correos masivos con archivos adjuntos maliciosos.

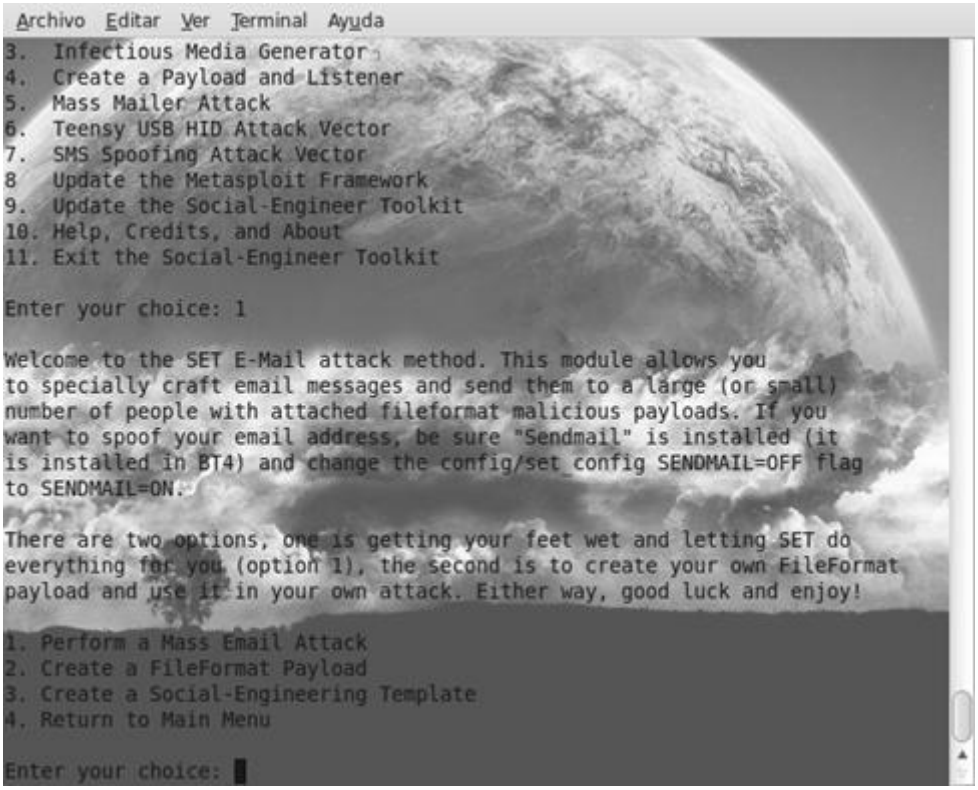


Figura 2.5 Opciones principales del SET

- Creación de medios infectados. Como se ve en la *Figura 2.6* el programa permite crear el fichero *autorun.inf* y un *payload* de *Metasploi*t. Al insertar el medio, sea este CD/DVD/USB se ejecutará automáticamente y posteriormente nos dará acceso a la máquina afectada.

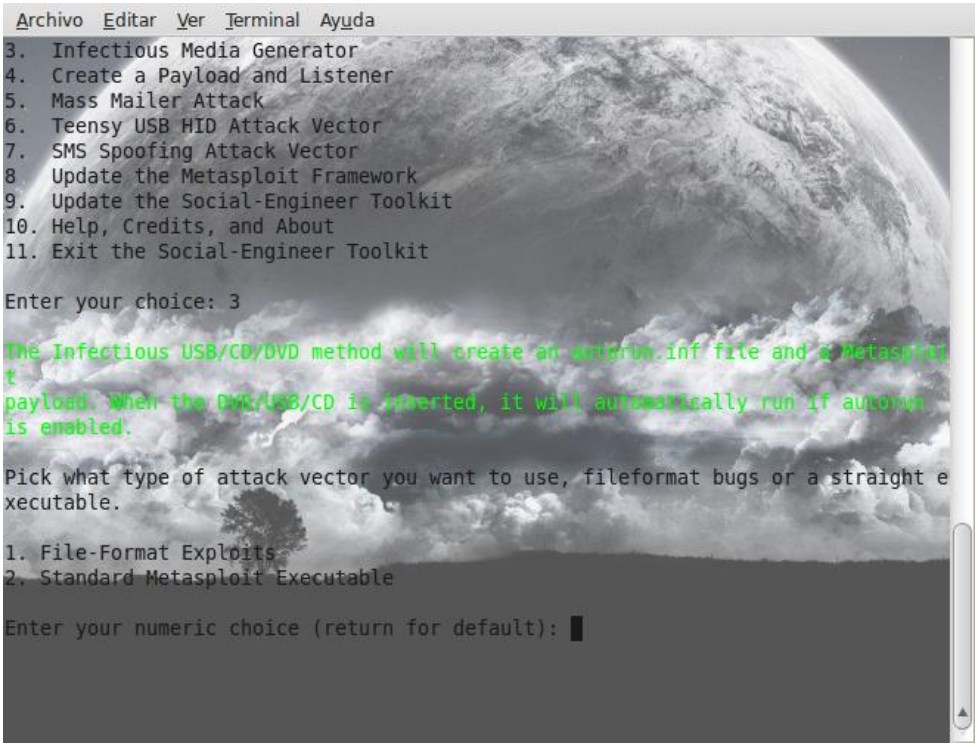


Figura 2.6 Creación de medios infecciosos

- *Falsificación de mensajes de texto (SMS).* Esta es una de las opciones más interesantes y eficientes del *SET*, como se muestra en la *Figura 2.7* pues nos permite enviar mensajes de texto falsos, suplantando el número telefónico del remitente, lo cual ayuda a la hora de hacerle creer al receptor que efectivamente ha sido enviado por esa persona o empresa.

  Además incluye la opción para el envío masivo de SMS sin problema. Las empresas prestadoras del servicio de envío de mensajes son: *SohoOS*, *Lleida.net*, *SMSGANG*. La única gratuita es SohoOS, y debido a esa característica en el mayor de los casos es limitada.

Figura 2.7 Falsificación de mensajes de texto

- *Interfaz Web*. Esta versión de *SET* ha integrado una fantástica interfaz web para lanzar cualquier tipo de ataque de una manera más cómoda e intuitiva. Esta opción se ilustra en la *Figura 2.8*

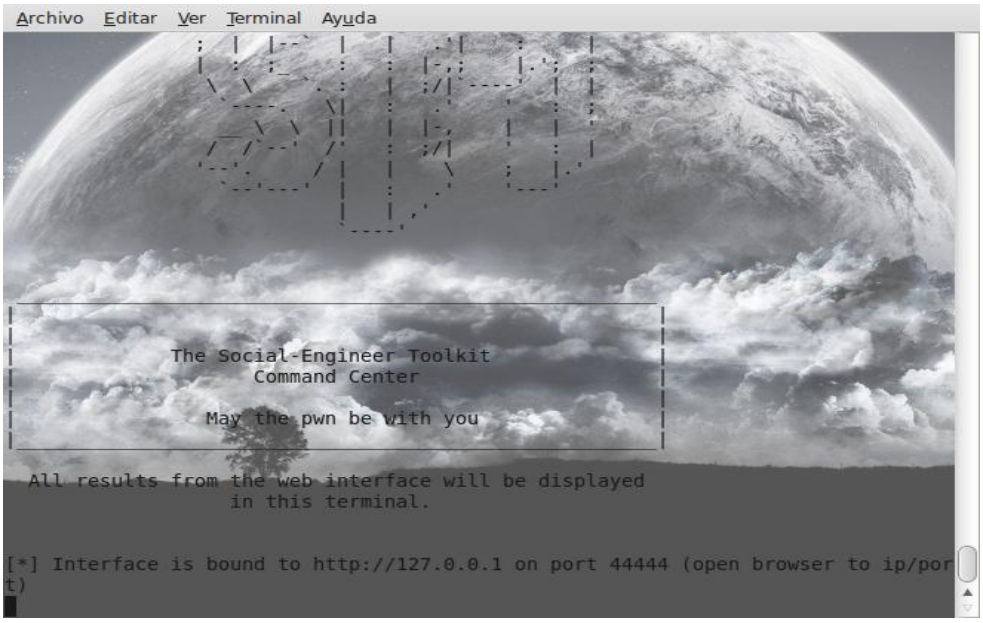


Figura 2.8 Interfaz web

Otro ejemplo de este es el *BaseKit* es el editor web más flexible e intuitivo del mundo. Te permite crear páginas web desde el navegador con sólo unos click. También puedes añadir funciones avanzadas sin mayor complicación. No se necesita conocimientos técnicos para crear una página. Además, tienes gran variedad de plantillas, videos de ayuda y un equipo de soporte para ayudarte en cada paso.

2.3.4- Keylogger (key (tecla), logger (registrador).

Es un programa o *software* espía que registra las pulsaciones que se realizan en el teclado, para posteriormente guardarlas en un archivo o enviarlas a través de internet a un correo pre designado por el atacante, se usa normalmente como *malware* permitiendo que otros usuarios tengan acceso a contraseñas importantes, algunos ejemplos son: contraseña de las tarjetas de crédito, contraseña de acceso a *Windows*, contraseñas de archivos, etc.

En este caso los registros se hacen con dispositivos de *hardware* y *software*, los sistemas disponibles incluyen dispositivos que pueden conectarse al cable del teclado y al teclado mismo.

Como cualquier programa puede ser distribuido a través de un *troyano* o como parte de un virus informático, para evitar este tipo de prácticas se utilizaban teclados virtuales ya que sólo requiere *click* del ratón, sin embargo, las aplicaciones más nuevas también registran *screenshots* al realizarse un click, que anulan la seguridad de esta medida, de igual forma los teclados *touch* eran una buena forma, pero incluso ahora los *keylogger* pueden identificar en que parte de la pantalla se tocó, con lo cual es difícil contrarrestar esta práctica.

Un *keylogger* tipo hardware como el que se muestra en la Figura 2.9 son dispositivos disponibles en el mercado que vienen en tres tipos:

- Adaptadores en línea que se intercalan en la conexión del teclado, tienen la ventaja de poder ser instalados inmediatamente. Sin embargo, mientras que pueden ser eventualmente inadvertidos se detectan fácilmente con una revisión visual detallada.

- Dispositivos que se pueden instalar dentro de los teclados estándares, requiere de habilidad para soldar y de tener acceso al teclado que se modificará. No son detectables a menos que se abra el cuerpo del teclado.
- Teclados reales del reemplazo que contienen el *Keylogger* ya integrado. Son virtualmente imperceptibles, a menos que se les busque específicamente.

Figura 2.9 Adaptador USB para conexión de teclado de Keylogger

Es simple de escribir, con un conocimiento básico de la *API* proporcionada por el sistema operativo objetivo. Los *keylogger* de *software* se dividen en:

- *Basado en núcleo:* Este método es el más difícil de escribir, y también de combatir. Tales *keyloggers* residen en el nivel del núcleo y son así prácticamente invisibles. Derriban el núcleo del sistema operativo y tienen casi siempre el acceso autorizado al *hardware* que los hace de gran alcance. Un *keylogger* que usa este método puede actuar como driver del teclado por ejemplo, y accede así a cualquier información registrada en el teclado mientras que va al sistema operativo.

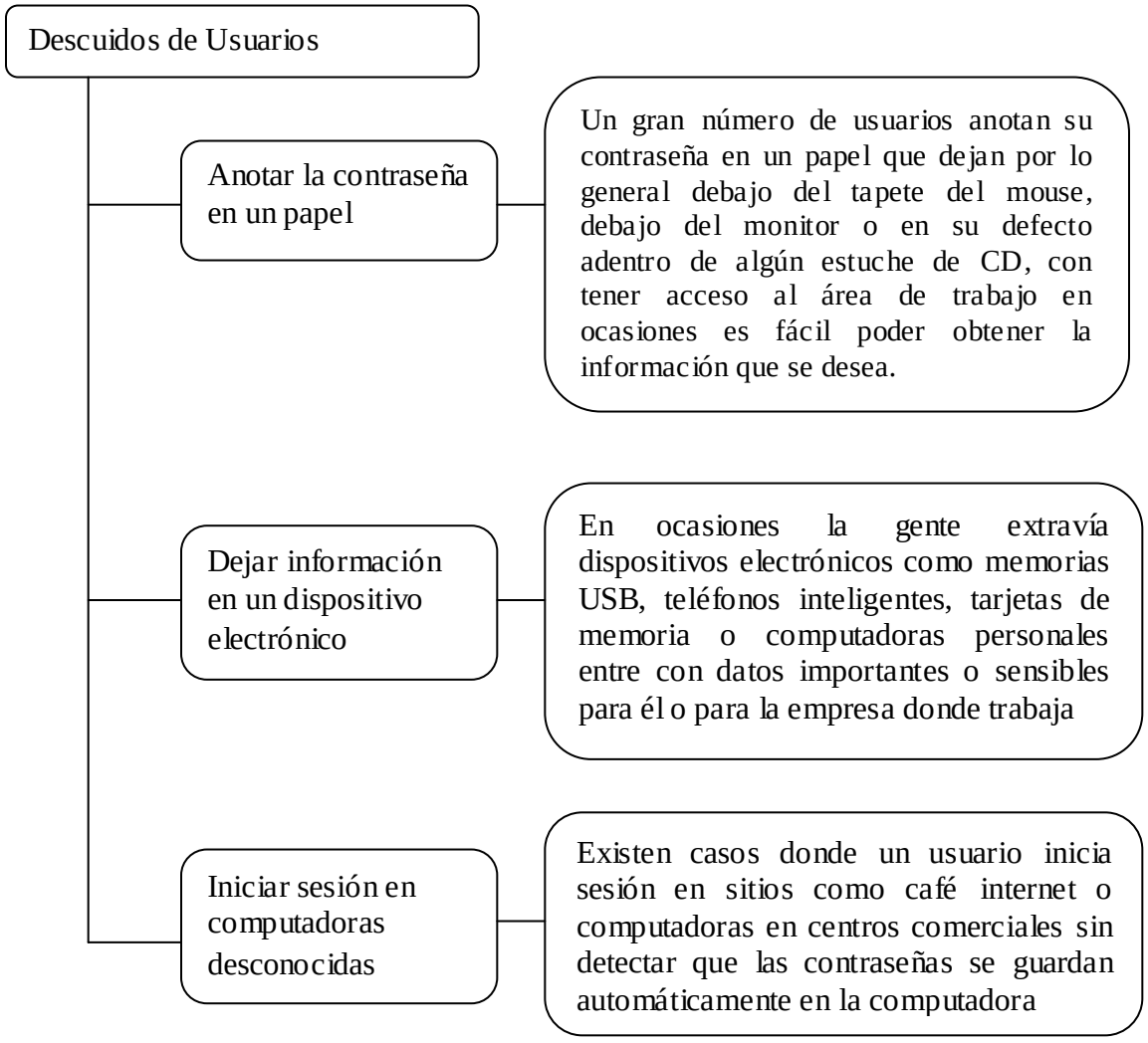
- *Enganchados:* Estos *keyloggers* registran las pulsaciones de las teclas del teclado con las funciones proporcionadas por el sistema operativo. El sistema operativo activa el *keylogger* en cualquier momento en que se presione una tecla, y realiza el registro.

- *Métodos creativos*: Aquí el programador utiliza funciones como *GetAsyncKeyState, GetForegroundWindow, etc*. Éstos son los más fáciles de escribir, pero como requieren la revisión el estado de cada tecla varias veces por segundo, pueden causar un aumento sensible en uso de la Unidad de Proceso Central (CPU) y pueden ocasionalmente dejar escapar algunas pulsaciones del teclado.

2.3.5- Descuido de los usuarios.

Otro método de *Phishing* existente es mucho más simple y se basa en la ingenuidad de los usuarios, debido a la gran diversidad de contraseñas que se usan actualmente, es difícil memorizarlas todas sobre todo cuando la gente tiene más de una y son diferentes.

Este método se basa en la observación del lugar de trabajo de los usuarios en ciertas ocasiones la mayoría de la gente escribe la contraseña y el usuario en algún papel o dispositivo electrónico que usan con frecuencia, ejemplos claros son los siguientes:



En la *Figura 2.10* tenemos un ejemplo de cómo es posible encontrar información debajo del tapete del mouse.

Figura 2.10 Ejemplo de contraseña debajo del tapete del mouse

2.3.6- Phishing por redes sociales.

Las redes sociales se han convertido en las vías más fáciles para obtener la información de los usuarios de estas mismas, los piratas informáticos han inundado Internet con correos electrónicos con basura y todos estos están plagados de virus en estas páginas tan populares en la actualidad tienen por blanco a los millones de usuarios estimados de *Facebook*, estos virus tienes la finalidad de robar las claves secretas de cuentas bancarias y otros datos delicados que se manejan en estos medios. Para conseguir esos datos, los mensajes informan a los usuarios de la popular red social que sus claves secretas han sido modificadas y que, para conseguir los nuevos permisos de inicio de sesión, deben abrir un archivo adjunto al texto. El adjunto está compuesto en realidad por varios tipos de software malicioso, incluido un programa que se roba las claves secretas.

2.3.7- Ofuscación de URL

Este método se basa en jugar con el localizador uniforme de recursos (*URL*). Una *URL* es una dirección que permite acceder a un archivo o recurso como ser páginas *html, php, asp*, o archivos *gif, jpg*, entre otros. Se trata de una cadena de caracteres que identifica cada recurso disponible en la web.

Se consiguen dominios con *URL* parecida a la de alguna página en internet como por ejemplo si se compra el dominio *liives.com* o se compra el dominio *loginlive-account.com* ahora se procede a diseñar un sub-dominio a nuestro dominio comprado.

http://msn.loginlive-account.com

Al hacer click este nos re direccionará a la página montada y no a la pagina original de MSN loggin.

http://msn.loginlive-account.com/windows/msn/messenger/connect/index.php

Se ha observado que este tipo de ataques de *Phishing* fueron ejecutados ampliamente cuando esta amenaza de Internet estaba en su fase inicial.

Algunos trucos para este método son los siguientes:

- *Uso de cadenas*. Utiliza una cadena de texto que suena creíble dentro de la *URL* Ejemplo: *http://XX.XX.43.102/ebay/account_update/now.php,* se puede observar que los dos primeros octetos de la dirección *IP* se han ocultado por razones de seguridad. Sin embargo, en un escenario en tiempo real esta apuntará hacia un servidor web *hosting* una pantalla de conexión falsa para su cuenta de *eBay*.

- *Usando símbolo* @. Este tipo de sintaxis se utiliza normalmente para los sitios web que requieran autenticación de algunos, sin embargo los hackers hacen uso de esta sintaxis para engañar a las víctimas a visitar una página de acceso falsa. Esto funciona en un concepto simple que en el contenido en la parte izquierda del símbolo @ se ignora y el nombre de dominio o dirección *IP* en el lado derecho del signo @ es entendido como el dominio legítimo.
  Ejemplo: *@http://www.citybank.com/update.pl xx.xx.43.102/usb/upd.pl*

- *Trucos de la barra de estado*. La *URL* es tan larga que no se puede mostrar por completo en la barra de estado, a menudo se combina con la @ para que la URL fraudulenta se encuentra al final y no se muestra lo que la víctima lo toma como un anfitrión legítimo y regala su información confidencial.

- *Trucos similares Nombre.* Este tipo de trucos utiliza un sonar creíble, pero el nombre fraudulento, de dominio. Este tipo de trucos han sido a menudo utilizado por los atacantes logren una ventaja psicológica sobre la víctima. Ejemplo: *http://www.ebay-support.com/verify, http://www.citybank-secure.com*/login- La *Figura 2.12* muestra el sitio web de *SunTrust Bank* Sin embargo la *Figura 2.11 www.suntrustbank.com* no es la página web de *SunTrust Bank Inc.*

Figura 2.11 Página no oficial de SunTrustbank

Figura 2.12 Página oficial de SunTrustbank

- *URL como truco botón:* La *URL* que se muestra está contenida en la descripción de texto de un botón de formulario. El mismo botón es el formato para que coincida con el fondo de correo electrónico de manera que sólo muestra el texto del botón, formulario de declaración, ya que sale la dirección *URL* falsa no aparece en la barra de estado del cliente de correo electrónico. Sin embargo, cuando se pone el ratón sobre el botón, el atacante utiliza el ratón sobre la etiqueta *HTML* para forjar el vínculo que aparece en la barra de estado.

- *Trucos redirección URL:* Utiliza la capacidad de reorientación de un proveedor conocido a enviar al usuario al sitio de *Phishing*. La redirección es utilizado por muchos sitios más grandes como *Yahoo, MSN, y Citibank*. Ejemplo: *http://r.aol.com/cgi/redir?http://www.ebay_secure.info/update_user*

- *Doble redireccionamiento Trucos:* Combina el sencillo método de redirección con un servicio de enmascaramiento *URL* como *tinyurl.com* o *cjb.net* El servicio de enmascaramiento asigna al usuario un alias para su dirección *UR*L. Ejemplo: *http://r.aol.com/cgi/redir?http://jne9rrfj4.CjB.neT/?uudzQYRgY1GNEn*
  Primero envía a: *http://r.aol.com/cgi/* y luego Redirigido a:
  http://jne9rrfj4.CjB.neT/?uudzQYRgY1GNEn (cjb.net)
  Redirigido a: lugar destinado a través del servicio de redirección de *cjb.net* La dirección *URL* real se almacena en *cjb.net* y se accede a través del alias *cjb.net*.

2.4- Robo de información de tarjetas bancarias

El robar información en la actualidad de la tarjeta bancaria es una práctica muy lucrativa y sencilla es por eso que se presenta mucho, un ejemplo claro de ello es el siguiente.

Los ladrones que roban la información de tu tarjeta de débito o crédito cuando usas el cajero automático se están convirtiendo en sofisticados criminales, utilizando lectores magnéticos escondidos en las ranuras de la máquina, así como teclados falsos para grabar la información que marcas, e inclusive diminutas cámaras escondidas que apuntan hacia el teclado y graban el movimiento de tus dedos para adquirir tu clave.

En muchos casos, la sofisticación de los criminales ha llegado al punto de diseñar los aparatos que utilizan para robar la información conforme a la marca del cajero automático o del banco que lo ofrece, de manera tal, que los colores y el diseño son idénticos a la máquina original, y por lo tanto casi imposible de detectar.

- *Teclados falsos.* Estos teclados como el que se muestra en la *Figura 2.13 y 2.14* son sobrepuestos a los teclados originales del cajero automático, pero su única función es grabar la secuencia de teclas pulsadas para marcar el número de identificación persona que te da acceso a tu cuenta bancaria.

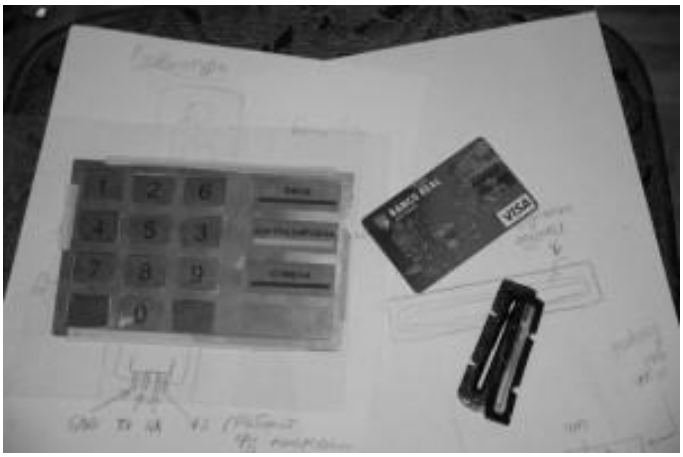


Figura 2.13 Teclado falso de cajero automático

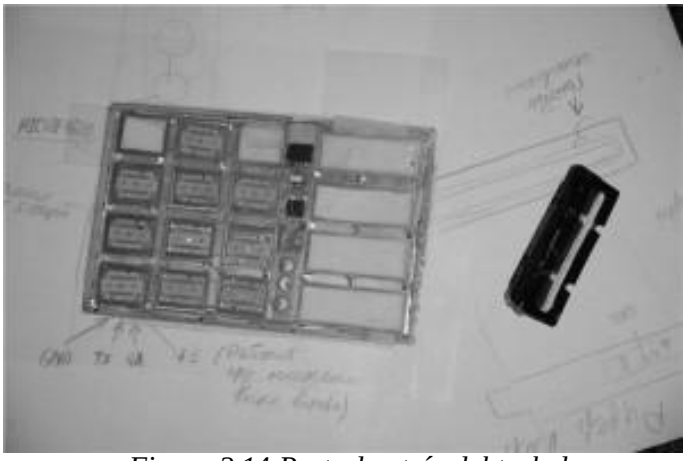


Figura 2.14 Parte de atrás del teclado

- *Lectores magnéticos falsos*. Estos lectores magnéticos conocidos en inglés como *Skimmers* son insertados encima del lector original, de forma tal que parecen ser parte del cajero automático. En realidad lo que hacen es leer toda la información contenida en la cinta magnética de tu tarjeta de crédito o débito. Esta información es luego duplicada en tarjetas falsas que utilizan para comprar productos o sacar dinero en el caso de las tarjetas de débito. En la *Figura 2.15* se muestra como es montado uno de estos lectores.

Figura 2.15 Lector magnético falso

- *Cajeros Automáticos Falsos.* Otra técnica que está muy de moda entre los criminales es comprar un cajero automático de segunda mano, los cuales cuestan alrededor de $800 dólares. Una vez que lo adquieren, entran en el sistema operativo de la máquina (*Windows XP* en su mayoría) e instalan un programa con una interface similar a los que aparecen en las máquinas reales, pero cuyo único propósito es grabar toda la información que el usuario produce para después crear tarjetas de crédito falsas. Cuando todo está listo, simplemente instalan el cajero automático falso en algún lugar con bastante tráfico de peatones y listo.

  En la mayoría de los casos, el usuario nunca se percata de que trató de sacar dinero de un cajero automático falso, ya que simplemente recibe un mensaje en la pantalla indicando que la transacción no pudo completarse.

- *Cámaras escondidas*. Los criminales utilizan unas cámaras diminutas escondidas en lugares estratégicos como lo muestra la *Figura 2.16*. Al igual que los teclados falsos, la idea es grabar tus manos mientras marcas tu número de identificación.

Figura 2.16 Cámaras ocultas en lugares estratégicos

2.5 Herramientas contra el *Phishing*

- *Prevención del usuario:* Algunas herramientas en contra del *Phishing* son realmente muy simples, estas se basan en que el usuario tenga cuidado a la hora de realizar trámites o usar su información personal, de la misma forma se debe de estar atento a las cosas que recibimos por correo electrónico y que no solicitamos o vienen de dudosa procedencia.

  Para ello es necesario:

  - *Estar atento a quien nos está enviando e-mail***s**. Se verifica de esta forma si quien nos está enviando correos es alguien de confianza y así poder ver la autenticidad de un correo electrónico.

  - *Es raro que un servicio web requiera que re-mandes tus datos***.** Es difícil que un banco solicite datos por internet, así como algunas las páginas de redes sociales. Sobre todo si no se ha pedido o reportado la perdida de los mismos.

- *Ante la duda, no hacer nada de lo que diga el e-mail.* Si realmente es importante hacer algo para algún servicio *web* que necesita los datos y se tiene dudas de la veracidad del correo es importante no seguir adelante y esperar a poderlo verificar de otra forma.

- *No tener tanta ingenuidad*. Aun que la gente piense que no puede pasar, en ocasiones los usuarios son tan ingenuos que revelan información personal con tan solo pedírselos, esto ocurre principalmente en redes sociales como el Messenger y Facebook, donde un usuario creado para esta práctica principalmente una imagen sugerente puede ser de una mujer o un hombre atractivos puedes ganarte la confianza de alguien a tal grado que con pedirle su información la proporcionarán sin ninguna sospecha o queja.

- *Tener instalada la última versión de tu navegador*: Es importante tener la última versión del navegador que se utiliza preferentemente, debido a que al tenerlo actualizado se corrigen varios errores presentes en ellos y de igual forma nos permite tener algunas funciones extras que nos ofrece para prevenir este tipo de problemas, esto lo realiza gracias a su sistemas de detección de este tipo de fraudes. Algunos navegadores te informan si el sitio al que se desea ingresar es de confianza o no, *firefox* por ejemplo desde su versión 2 nos proporciona automáticamente una protección contra el *Phishing*, trabaja comprobando los sitios a los que entras con a una lista de sitios *Phishing* conocidos. La lista se descarga de manera automática y se pone al día regularmente. Otro ejemplo más actual es *Google Chrome* en este caso nos avisa a través de la tecnología de navegación segura de *Google* si el sitio al que estás intentando acceder es sospechoso de practicar la suplantación de identidad o de instalar software malintencionado en nuestro equipo, en este caso se nos avisa de la siguiente manera:

  - *Advertencia: Algo fallo aquí***.** Este mensaje aparece cuando *Google Chrome* detecta que el sitio al que se quiere acceder puede tener software malintencionado.
  - *Advertencia: Posible sitio de Phishing***.** Este mensaje aparece si se detecta que el sitio al que se intenta acceder puede ser un sitio que realiza prácticas de suplantación de identidad.

- *Realizar un chequeo rápido de los dispositivos que usamos.* Una de las formas más prácticas para evitar el *Phishing* es dar un pequeño chequeo del aparato que estamos utilizando, como se ha mencionad algunos *keyloggers* se conectan a una parte del teclado y con un pequeño vistazo es fácil detectarlos, en el caso de los cajeros automáticos intentar forzar la ranura del lector de tarjeta nos permite observar si está montado un dispositivo ajeno al cajero automático que se utiliza. De igual forma es importante que cuando utilicemos un equipo ajeno al nuestro dediquemos un tiempo a observar que no dejemos información personal en el mismo, se presentan algunos casos donde al "loguearnos" en alguna página de red social o en nuestra página bancaria, no dejemos nuestra sesión de usuario abierta, ya que de esta forma nos pueden quitar nuestra información personal aunque parezca en ejemplo absurdo es muy fácil que ocurra.

- *Conocer y aprender a utilizar nuestro servicio de correo electrónico*. En la actualidad es importante saber las diversas ventajas y desventajas de usar algunos servicios de correo electrónico, debido a que algunos de ellos nos ofrecen una gran variedad de herramientas y protección contra este tipo de amenazas, un ejemplo clave es el siguiente:

  Google incluyó mejoras para su servicio de correo electrónico gratuito, *Gmail***,** y se trata de una protección contra emails que traten de suplantar la identidad de comunicados de las empresas *Ebay* y *Paypal*. Funciona con los mensajes que intentan simular la procedencia del popular sitio de subastas *eBay* y del sistema de pago *PayPal*. El sistema de autenticación que utiliza es *DomainKeys*, y todos los emails procedentes que no lleven la firma serán bloqueados por *Gmail* directamente la firma digital se muestra en la *Figura 2.17*.

Figura 2.17 Ejemplo de firma digital de eBay en Gmail

Esta nueva función puede habilitarse desde *Gmail*, accediendo a Configuración y después a la pestaña *Labs*. La función se llama Icono de autenticación para remitentes verificados y se muestra en la *Figura 2.18***.**

Figura 2.18 Icono de autenticación para remitentes verificados

Los usuarios que abrían el email era redirigidos a una *web* externa a *PayPal*, donde introducían sus datos personales y contraseña. Como en otros casos de *Phishing* el funcionamiento era sencillo, una vez conseguidas las claves en una *web* como cebo donde apenas funcionaba un formulario, los datos privados se enviaban a una cuenta donde los estafadores utilizaban las claves para sacar el dinero de las carteras virtuales. La dificultad que tiene esta herramienta para tener éxito es que depende de una base de datos de dominios fraudulentos donde se instalan las webs trampa donde enlazan los correos de *Phishing*.

- *Barra de protección para el navegador*. En la actualidad existen nuevas formas de poder proteger nuestra información al momento de navegar en internet de las más recientes y son las barras de navegación, las cuales evitan que se entre a sitios riesgosos, existen una gran cantidad de barras de herramientas (*toolbars*) que permiten evitar páginas fraudulentas, de igual forma bloquean la publicidad y estas tienen información sobre las páginas que visitas, para poder evitar riesgos al momento de navegar en internet.

Estas son muy útiles, por ejemplo, si se realizan compras en páginas web del extranjero ya que indica: el país en donde se encuentra la página, su fecha de creación, etc. Hay varios complementos que sirven para proteger nuestro navegador, aunque no es recomendable instalarlos todos para que no haya problemas con el rendimiento de nuestro equipo.

Ejemplos de estos complementos son los siguientes:

a) *WOT***.** Web de Confianza (en ingles *Web Of Trust*) es un complemento compatible con *Firefox*, *Internet Explorer* y *Google Chrome*, cada vez que se realice una búsqueda o visites un sitio web, nos indicará si el sitio es fiable o no.

b) *Netcraft***.** Esta barra de herramientas utiliza la base de datos de *Netcraft* para obtener información útil que permita identificar los sitios falsos. Muestra la localización del *hosting*, la empresa propietaria de la dirección *IP*, e incluso la fecha de creación.

c) *Link Extend***.** Esta extensión para *Firefox* reagrupa diferentes barras de búsqueda y otros módulos de protección *antiPhishin*g, es práctica y cuenta con bastante información, el único inconveniente que tiene es que es un poco compleja para los principiantes.

d) *Mcafee Site Advisor***.** Esta herramienta te protege contra las amenazas en línea como los programas espías y el *Phishing*.

e) *Trend Protect***.** Es un complemento que ayuda a evitar las páginas web con contenido indeseable. En función de esta evaluación, podrás decidir si deseas consultar la página en cuestión o evitarla. Para la evaluación de las páginas web, Trend Protect utiliza una base de datos detallada que proporciona la siguiente información acerca de las páginas web:

- Categoría del contenido.
- Detección de estafas de *Phishing*.

- Reputación del sitio web.
- Reputación de la página.

f) AVg link scanner:

- Evita las páginas web infectadas
- Notas de seguridad precisas para los resultados de búsqueda en Google, MSN y Yahoo.
- Compatible con todos los antivirus y programas de seguridad más populares.
- Analiza las páginas una por una, no sitios, lo que le permite acceder a un sitio incluso si una de las páginas está contaminada.
- Analiza las páginas web en tiempo real, en el momento en que realmente importa es decir cuando se hace clic sobre un enlace.
- Fácil de instalar y ejecutar y no ralentiza el sistema.

g) *SpoofStick***.** Es una barra de herramientas para *Internet Explorer* y *Firefox*. Informa al usuario sobre la dirección real del sitio web que visita lo que permite evitar cualquier fraude por *Phishing*.

Y algunas de las barras más conocidas como son:

h) *Google Toolbar***.** Es una barra de herramientas que permite comprobar si un sitio web es fraudulento, esta barra se basa en la lista negra de *Google*.

i) *Yahoo Toolbar*. Permite bloquear la publicidad y posee un antispyware.

- *Uso de aplicaciones web que permite identificar posible malware, Phishing, o algún que otro virus.* Una práctica eficiente para poder saber si le sitio *web* al que se quiere acceder es de confianza o no es analizar la página por medio de algunas aplicaciones *web*, esta nos permitirán saber si la página en cuestión tiene algún *malware* o *Phishing* que nos pueda afectar, una página comúnmente usada es:

- *URLVoid*. Este es un servicio online, el cual analiza si una página web es segura o no, escanea la *URL* que proporcionemos en busca de todo tipo de virus. En forma bien sencilla, para analizar un sitio *web*, sólo hay que pegar al dirección *URL* en *Insert site to check* y dar click en "*Scan Now*" como lo muestra la Figura 2.19. En dicho análisis, se puede ver si se encuentra en estado limpio o sospechoso, también se pueden ver datos como el *Hash MD5*, dirección *IP*, *IP* del host, país, el porcentaje de detecciones, entre otras cosas como lo muestra la *Figura 2.20 y 2.21*.

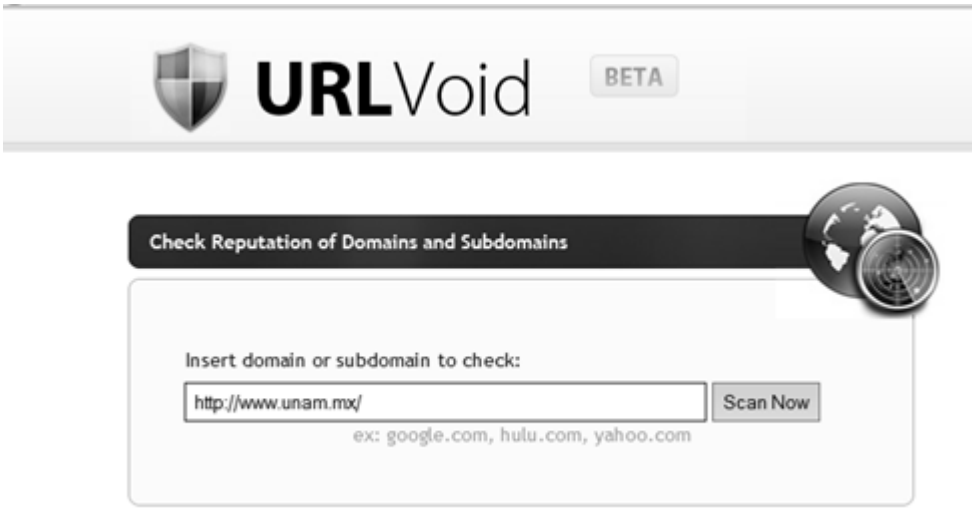


Figura 2.19 Sistema de URLVoid escaneando la página de la UNAM

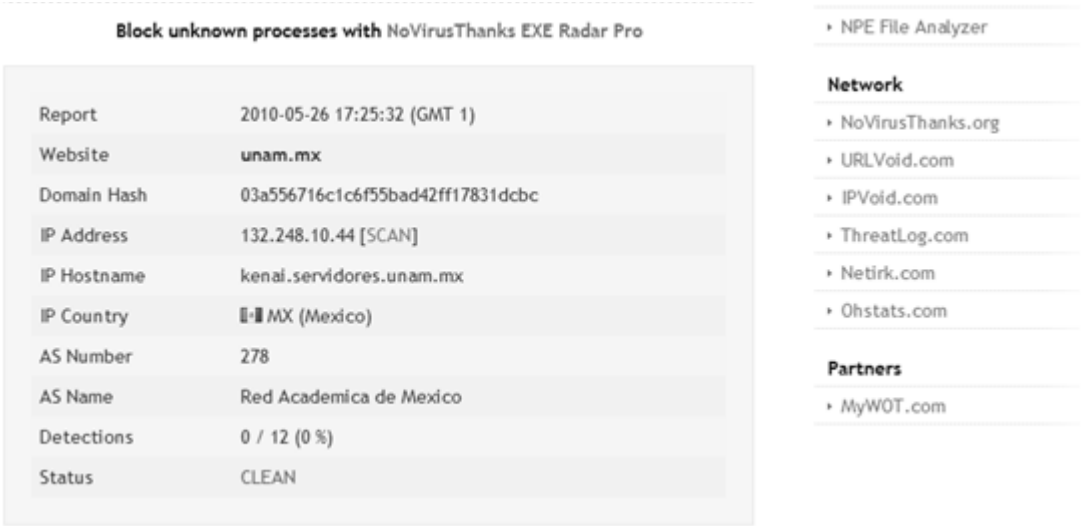


Figura 2.20 Reporte de URLVoid con el resultado de la página de la UNAM

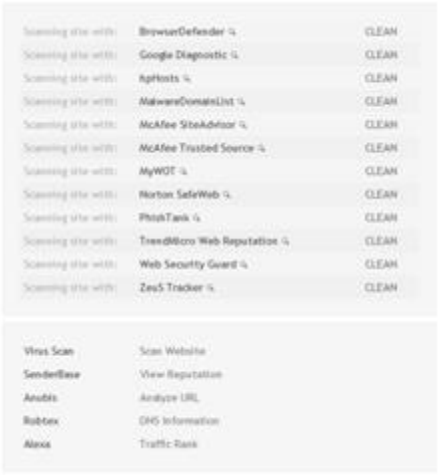


Figura 2.21 Reporte con el escaneo de diversos sitios web

- *Antivirus.* Es importante tener un buen antivirus que proporcione protección, es importante que nuestro antivirus este actualizado para evitar fallas que tengan o alguna vulnerabilidad que pueda explotar algún hacker. Algunos antivirus tienen una protección especial contra el *Phishing*, esto lo ofrecen casi todos los antivirus. Los antivirus tienen su propia protección en línea con su versión *internet security*, brindan una función llamada *Anti-Phishing* el cual asegura que las páginas *web* sean realmente lo que parecen ser. También ofrecen un componente *Web Shield* el cual comprueba cada página cuando hace clic en el vínculo para garantizar que no le ataque ninguna descarga dirigida furtiva ni cualquier otro abuso.

  Se analizan todos los vínculos de los resultados de búsquedas de *Google, Yahoo y MSN* y se informa de su nivel de amenaza actual en tiempo real antes de hacer clic en el vínculo y visitar el sitio. Otras funciones de los antivirus son los filtros *antispam*, el cual detecta los correos electrónicos de *Phishing* y, en el mejor de los casos no los admite.

  Con la técnica de *OutbreakShield,* aplica el filtro de *spam* más eficaz protegiéndole en tiempo real de todo tipo de correos *spam* y *Phishing*_independientemente de su contenido. La mayoría de estos antivirus funcionan en todos los sistemas operativos y casi todos cuentan con una versión gratuita que si bien no nos ofrece la mejor protección y más completa, nos brinda protección contra códigos maliciosos y no brinda protección adicional a las amenazas del internet.

2.6- Organizaciones encargadas de combatir el Phishing

Existen organizaciones especializadas en el combate contra el Phishing, estas organizaciones se encargan de revisar el código fuente de las páginas de internet que los usuarios reportan como páginas con posibles amenazas o fraudulentas, un ejemplo muy representativo es la *Subdirección de Seguridad de la Información* y *Servicios de Seguridad en Cómputo de la Universidad Nacional Autónoma de México* o el *Anti Phishing Working Group (APWG).*

La Subdirección de Seguridad de la Información/UNAM-CERT, perteneciente a la Dirección General de Cómputo y de Tecnologías de Información y Comunicación; se encarga de establecer políticas de seguridad adecuadas, disminuir la cantidad y gravedad de los problemas de seguridad informática y difundir la cultura de la seguridad en cómputo.

En esta página ofrece una serie de noticias, alertas, boletines, servicios, sección de reportes para usuarios, artículos y documentos, así como muchas otras funciones. Esta página no brinda una sección de reportes de *Phishing* donde se pueden reportar los incidentes mediante su portal[1] con los siguientes datos:

- Encabezados del correo malicioso.
- Correo sospechoso original.
- URL del sitio sospechoso.

Para reportar cualquier otro incidente de seguridad informática ponen a nuestra disposición una dirección de incidentes: incidentes@seguridad.unam.mx

Incluya en el mensaje:

- Su información de contacto.
- Descripción del incidente.
- Direcciones IP y/o nombres de host o dominio involucrados.

[1] http://www.seguridad.unam.mx/index.html, obtenido en Diciembre del 2011

CAPÍTULO III

CASOS DE ESTUDIO, INTERPRETACIÓN DE ESTADÍSTICAS Y TENDENCIAS

En este capítulo se analizaran las tendencias que siguen los Ingenieros Sociales para llevar a cabo sus prácticas.

CAPÍTULO III CASOS DE ESTUDIO, INTERPRETACIÓN DE ESTADÍSTICAS Y TENDENCIAS

3.1- Casos de estudio

Para demostrar las tendencias que sigue el *Phishing* se analizaran 10 noticas relacionadas con *Phishing* para poder observar que es técnica es la más utilizada, las noticias presentadas son del mes de noviembre del 2010 al mes de octubre del 2011.

3.1.1- Phishing de Facebook con mensajes directos falsos[1]

El siguiente caso de Phishing busca robar la contraseña de *Facebook*, como se puede ver en la *Figura 3.1*, primero se recibe un correo que simula ser un mensaje privado y luego se carga una página fraudulenta:

Figura 3.1 Correo falso que simula ser enviado por Facebook

[1] SpamLoco.net (10/2011). *Phishing de Facebook con mensajes directos falsos.* http://spamloco.net/2011/10/Phishing-de-facebook-con-mensajes.html. Fecha de acceso noviembre del 2011

El enlace muestra claramente que el destino es una página sospechosa, el dominio es un parámetro *.co.cc*, con el cual se puede registrar de forma gratuita y suele ser utilizados para esta clase de ataques. De hecho, los *spammers* y *ciberdelincuentes* abusaron tanto de la extensión que *Google* la terminó eliminado de su índice. Pero la mayoría de los usuarios no saben esto y como el dominio contiene las palabras facebook.login podrían ser engañados, sin embargo hay otros detalles que deberían levantar sospechas. El mensaje no es enviado por *Facebook* sino desde un correo de Hotmail y además contiene faltas de ortografía como la palabra "*atravez*" en el Asunto y el nombre "*Gracia*" en el remitente, distinto al que contiene el mensaje.

Si se hace clic en el botón se termina en una página que solicita iniciar sesión, como se puede ver en la *Figura 3.2* su diseño es similar al *de Facebook*, pero al ingresar los datos en realidad se envían al atacante. Luego se realiza una redirección hacia *www.facebook.com/login.php* que sería la misma página, pero real:

Es importante no olvidar verificar siempre las *URLs* de las páginas antes de ingresar tus datos. Si un correo parece sospechoso, lo mejor es ignorarlo y buscar ayuda para saber si es real o no.

Figura 3.2 Página falsa de Facebook

3.1.2- Severo ataque de Phishing en Twitter.[2]

Naked Security, el blog de *Sophos*, informa que se está llevando a cabo un ataque de *Phishing* en *Twitter* el cuál si el usuario no está alerta, puede llegar a entregar credenciales de *Twitter* a los atacantes. Varios usuarios reportaron haber recibido mensajes directos (*DM*) preguntándoles si ellos eran los que mencionaban en un video, fotografía o en el post de un blog. El *DM* viene con un enlace.

Los mensajes incluyen los siguientes textos:

- *¿Este es tu video?*
- *¿Esta es tu foto?*
- *Checa esto…. es un blog muy gracioso. Tu lo mencionaste*

El equipo de seguridad de *Twitter* está alerta de este problema y está cambiando las contraseñas de los usuarios que cree fueron atacados. En la *Figura 3.3* se puede apreciar que la dirección no es de la oficial de la página de *Twitter*. Mientras que en la *Figura 3.4* podemos ver la página la similitud de que tiene esta página con la oficial de Twitter.

Figura 3.3 Dirección falsa para el login de Twitter

[2]NakedSecurity(10/Julio/2011). Twitter phishing attack spreads via Direct Messages. http://nakedsecurity.sophos.com/2011/07/09/twitter-phishing-attack-spreads-via-direct-messages/. Fecha de acceso noviembre del 2011

Figura 3.4 Página similar de Twitter

Si se conectan estarán entregando su nombre de usuario y password a los atacantes. El equipo de seguridad de Twitter está alerta de este problema y está cambiando las contraseñas de los usuarios que cree fueron atacados.

3.1.3- Nuevo ataque de Phishing dirigido contra la Dirección General de Tráfico.[3]

Sophos acaba de dar la voz de alarme: existe un ataque de *Phishing* que se dirige contra la Dirección General de Tráfico (DGT), con el objetivo de conseguir datos personales de los usuarios, y que ya ha empezado a registrar las primeras víctimas de este engaño. "Este nuevo intento de suplantación de identidad, que ya ha sido reportado a las autoridades, se basa en una campaña de spam en la que avisan al usuario e que le han impuesto una sanción, con el objetivo de que rellenen el documento de *Word* y faciliten sus datos personales y los envíen a una dirección de correo de *Hotmail*. También incluyen un enlace a la web de la DGT para dar una imagen de veracidad", afirman desde la DGT.

[3](19/Enero/2011).http://www.muycomputerpro.com/2011/01/19/nuevo-ataque-de-Phishing-dirigido-contra-la-direccion-general-de-trafico/.Fecha de acceso noviembre del 2011

*"El spam, además, incluye un documento .pdf con una supuesta notificación de sanción, un documento Word de alegaciones y un acuse de recibo de correos. Es en este falso documento de alegaciones donde solicitan los datos personales de los usuarios como nombre, apellidos, dirección y número de DNI. Incluso se solicitan los mismos datos en caso de que hubiese testigos. "*A pesar de que parezca extraño que la DGT, envíe un email desde una dirección de Hotmail, ha habido usuarios que han caído en el engaño. Desde Sophos recomendamos la mayor precaución siempre que nos soliciten los datos personales y recordamos a los internautas que *se puede denunciar a las autoridades competentes todo aquello que consideren sospechoso", comentó Pablo Teijeira, Corporate Account Manager de Sophos Iberia."*

*El Phishing, en aumento. Durante el año 2010, la DGT, en el marco de la reforma de tráfico, ha creado numerosos portales telemáticos para que el usuario pueda comunicarse con este organismo. Utilizando estas novedades y aprovechando la falta de conocimientos de algunos usuarios, los casos de Phishing están aumentando en los últimos meses. "*Este Phishing basado en campañas de spam probablemente haya sido enviado desde ordenadores secuestrados sin que los propietarios sean conscientes de ello. Es *un tipo de amenazas que se empieza a extender en España* y debemos estar más alerta que nunca*", concluyó Teijeira.*

De hecho, como alertaba recientemente Sophos, España es el único país europeo, junto con Italia, en donde se registra una subida en el porcentaje como productor de spam en el último trimestre de 2010 con respecto a otros anteriores. Esto es una mala noticia y, más si tenemos en cuenta que este dato en Europa, como continente, ha bajado durante los últimos tres meses.

En la *Figura 3.5* se puede observar la gran elaboración del correo con la falsa sanción para que el usuario no perciba ninguna especie de engaño y así obtener sus datos personales.

Según lo atendido en el Registro Virtual de Infracciones (RVI), su cuenta de correo activa, corresponde al nº 399472 , de la Secretaría Virtual de Tráfico, desglosada en el archivo paralelo de la Dirección General de Tráfico, bajo la autorización de datos según el R.D 2008/43, por el que se determina la permisión de identidad en los apartados 3.2 y 6.6.3 de la Ley General de Integridad de datos (LGID).
Se le informa, que a fecha del 27-12-2010, en el RVI queda interpuesta la resolución por competencia sancionadora, por un valor en deuda de 150€ , a cargo de imputación de la obligación de adecuar la velocidad a tramo de vía convencional.

Las resoluciones dictadas por el órgano que tiene atribuida la competencia sancionadora pueden impugnarse mediante recurso en el plazo de un mes , conferido por el órgano instructor del procedimiento para que alegue cuanto considere conveniente a su defensa y proponga las pruebas que considere oportunas. Ello conforme al art.12.1 Reglamento del Procedimiento Sancionador en Materia de Tráfico, aprobado por el RD 320/1994 de 25 de febrero, teniendo en cuenta las modificaciones introducidas por el RD 318/2003 de 14 de marzo. El presente escrito de deuda procede cuando se haya imputado infracción de la obligación de adecuar la velocidad a las circunstancias. Le adjuntamos el modelo de **ESCRITO DE ALEGACIONES Y PROPOSICIÓN DE PRUEBAS CUANDO SE IMPUTA LA INFRACCIÓN DE LA OBLIGACIÓN DE NO REBASAR LA VELOCIDAD MÁXIMA PERMITIDA**, para cumplir su derecho de alegación pertinente.

Para su disponibilidad, queda archivado en nuestra base de datos el documento nº 399472, y el duplicado de envío de atención, para que a efectos legales quede contemplado el aviso de infracción y deuda correspondiente.
Para cualquier tipo de duda y el discurro del procedimiento, póngase en contacto con nosotros enviando sus alegaciones en Secretaria.Virtual.de.Trafico@hotmail.com o visitando el siguiente enlace: http://www.dgt.es/portal/ca/oficina_virtual/multas/

Atentamente el Registro Virtual de Infracciones.

Figura 3.5 Falso correo de sanciones

3.1.4- PayPal Phishing.[4]

Éste es un ejemplo ordinario de suplantación de identidad, en éste caso se utiliza a la empresa de pagos electrónicos *PayPa*l.
Si cayéramos en la trampa, los datos de acceso a nuestra cuenta PayPal pasarían a venderse en el "mercado negro" (en el mejor de los casos). Como curiosidad alentadora, si fuésemos víctima de éste Phishing y accediéramos al sitio PayPal falso y cambiáramos de idioma antes de introducir las credenciales, seríamos automáticamente re direccionados al sitio legítimo de PayPal sin realizarse el steal de datos. La web se encuentra activa aunque ya ha sido reportada, pero algunos navegadores web (Safari) no bloquean el acceso si no disponen de algún plugin adicional para tal fin.

[4] (10/octubre/2011). http://luctus.es/2011/10/paypal-Phishing/. Fecha de acceso noviembre del 2011

En la *Figura 3.6* se puede observar que la dirección falsa de *PayPal* y la gran elaboración de la página para poder convencer a los usuarios.

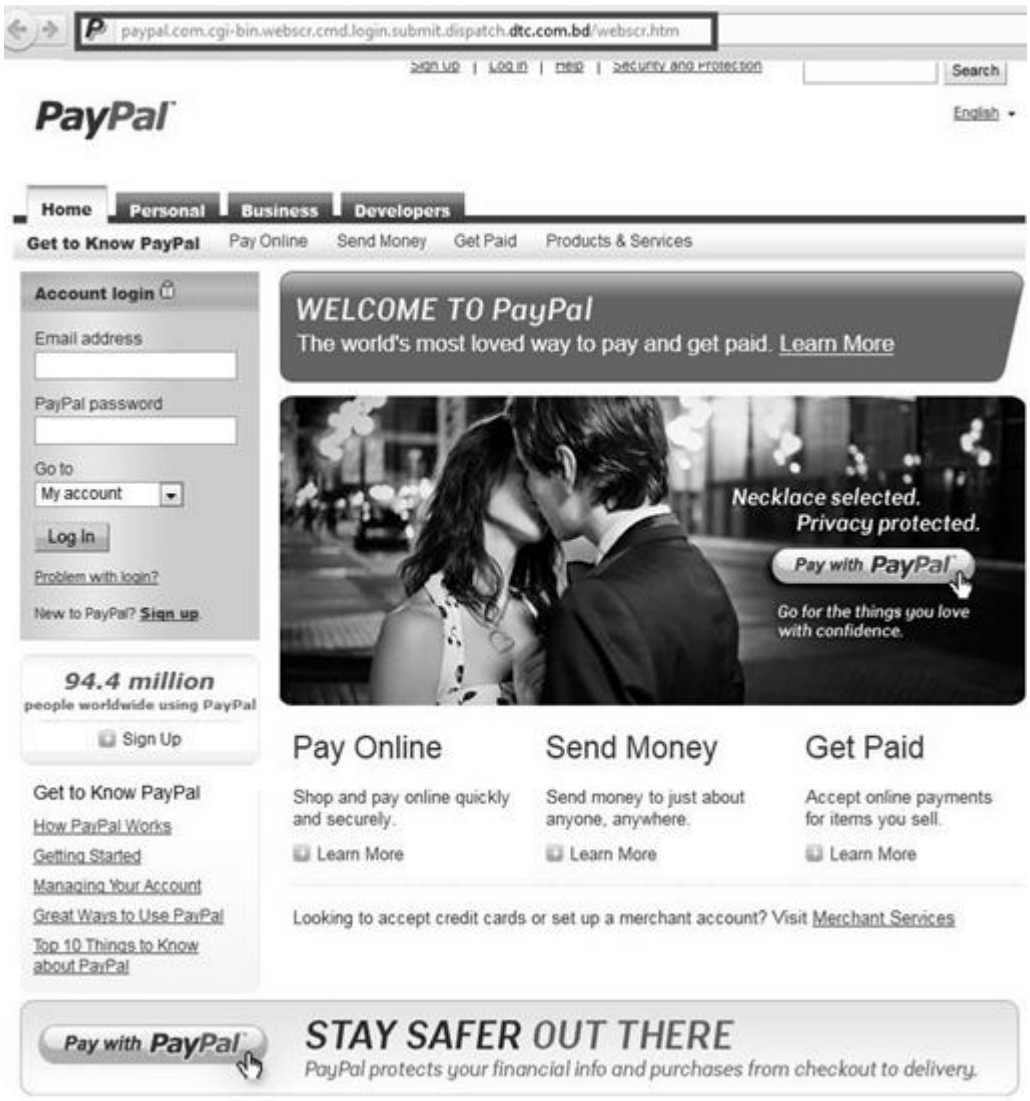


Figura 3.6 Portal falso de Paypal

3.1.5- Falsa aplicación de Netflix roba datos de usuarios.[5]

La plataforma de teléfonos móviles Android nuevamente amenazada con una aplicación de Netflix falsa que causaría la perdida de información de las cuentas. Se trata de una variable de Phishing, pero en vez de tratarse de una página web que suplante la identidad del sitio, llega en forma de aplicación móvil. Aprovechando la fama que ha alcanzado el sitio de vídeo streaming Netflix, y su reciente lanzamiento al habla hispana, usuarios malintencionados están distribuyendo la mencionada aplicación. Recordemos que la técnica de Phishing consiste en variadas técnicas para obtener los datos de cuentas de forma engañosa.

En esta ocasión el engaño llega ejecutando la aplicación de *Netflix*. Encontramos una ventana de bienvenida y de inicio de sesión. Al cargar el usuario y contraseña, los datos son enviados a un servidor remoto desconocido. Como siempre los datos son aprovechados para acceder a nuestras cuentas, y robar la información. El riesgo aumenta en caso de tener una membrecía paga, ya que datos de tarjetas o modos de pago pueden estar almacenados aun. *Como siempre, solicitamos a nuestros lectores que tomen las medidas correspondientes para evitar caer en la trampa de hackers. En este caso usar siempre la tienda oficial: Android Market. En caso de estar interesados en el popular servicio de películas y series ingresar al sitio oficial de Netflix*.

3.1.6- Los soldados norteamericanos son las nuevas víctimas del "Phishing".[6]

La reciente baja del troyano *Zeus* como principal móvil de las amenazas presentes en la Web ha logrado que los cibercriminales vuelvan su mirada sobre las técnicas de *"Phishing"*.

[5](14/octubre/2011).http://antivirus.es/falsa-aplicacion-de-netflix-roba-datos-de-usuarios-4081. Fecha de acceso noviembre del 2011

[6](3/noviembre/2010). http://antivirus.es/los-soldados-norteamericanos-son-las-nuevas-victimas-del-%e2%80%9cPhishing%e2%80%9d-3211. Fecha de acceso noviembre del 2011

En esta ocasión, han elegido como nuevas víctimas a los miembros actuales y retirados del ejército de EEUU. La estafa consiste en el envío de correos electrónicos que utilizan como remitente (falso, por supuesto) al *USAA*, entidad financiera que ofrece sus servicios a los soldados norteamericanos y a sus respectivas familias, desde préstamos hasta depósitos bancarios.

A través del cuerpo del mail, se conduce a la víctima hasta un enlace malicioso que la dirige a un sitio que emula a la perfección el portal oficial de "*United Services Automobile Association*" (USAA). Allí se le solicita que se llene un formulario con los datos correspondientes al nombre del cliente, número de tarjeta, y contraseña. *AppRiver*, la firma de seguridad que detectó estos ataques, ha logrado bloquear más de 1.500 dominios hasta el momento con este tipo de solicitudes, pero a la vez recuerda a los usuarios de servicios financieros que las entidades que los ofrecen nunca les solicitarán sus datos personales a través de correo electrónico.

3.1.7- Cuidado con StalTrak, nuevo fraude en Twitter.[7]

Continuamos con las alertas y protecciones sobre la red social de mensajes cortos. ¿Cuántas veces viste en Facebook la frase: "Mira quien ha visitado tu perfil"*? Este conocido modo de* Phishing*, ahora ha llegado a Twitter. Una nueva aplicación llamada StalTrak está dando voces de alerta entre los "twitteros". La misma ha sido diseñada para robar identidades y está haciendo* spam *entre los estados.*

Con algunos mensajes como: "descubre quien ha visitado tu perfil más veces" o "descubre quien te acosa por Twitter", el software intenta aprovecharse de las personas que menos conocimientos tienen en la red social. El texto incluye un enlace corto (por lo que se hace más difícil bloquear la dirección), en el cual se ofrece la instalación de la aplicación mencionada.

[7] (2/agosto/2011). http://antivirus.es/cuidado-con-staltrak-nuevo-fraude-en-twitter-3671. Fecha de acceso noviembre del 2011

La "utilidad" maliciosa adjudicará permisos para acceder a tu cuenta de Twitter, tus seguidores, a quienes sigues y también publicar en tu nombre. Una vez aceptado esto, solicita tu usuario y contraseña de la red de microblogging*. Para que la víctima no sospeche de que sus datos han sido ultrajados, se mostrará una ventana con las personas que sigue pero que no siguen a ella. De esta manera, tardará más tiempo en darse cuenta de lo sucedido. Recomendación: Ir a tu cuenta y revocar los permisos de acceso de StalTrak. Además, cambiar tu contraseña urgentemente, ya que los creadores de esta infección pueden seguir accediendo*.

Como se aprecia en la *Figura 3.7* esta aplicación parece totalmente segura debido a la gran forma de elaborarla y hacerla parecer como tal.

Figura 3.7 Imagen de autorización de la aplicación StalTrak

3.1.8- Vishing: Phishing a través de tecnología VoIP.[8]

Ahora los usuarios de Skype y de todos los servicios de comunicaciones por VOIP deberán prestar especial atención cuando estén en línea. Una nueva oleada de phishers *están comenzando a explotar este nuevo campo de acción para llevar adelante sus tretas. Durante el mes de abril, varios adeptos al popular software Skype han reportado llamadas no identificadas que informaban que su ordenador se encontraba infectado por malware, induciéndolos a ingresar en un sitio web para proceder a la desinfección*.

[8] (10/Mayo/2011). http://antivirus.es/vishing-Phishing-a-traves-de-tecnologia-voip-3384. Fecha de acceso noviembre del 2011

*Como muchos ya irán sospechando, en la mencionada página de Internet aguarda un rogueware, es decir un falso antivirus que corroborará el diagnóstico de la "misteriosa" llamada telefónica y buscará cobrar al usuario por llevar a cabo la desinfección del equipo. Dado a que seguramente no será la última vez que escuchemos hablar del "V*ishing*", es recomendable cambiar la configuración de los servicios VoIP para recibir llamadas únicamente de usuarios listados.*

3.1.9- Los cibercriminales utilizan a McDonalds como gancho para hacer Phishing.[9]

El Phishing llega a la comida rápida. El "I´m loving it"de McDonalds también gusta a los cibercriminales que han comenzado a usar esta compañía americana como gancho para sus estafas, advierte Kaspersky Lab. Expertos de Kaspersky Lab han detectado el envío masivo de un correo electrónico que, a primera vista, parece que ha sido enviado por McDonald´s.

En este correo se informa al destinatario de que ha sido seleccionado para participar en una encuesta y que una vez contestadas las preguntas recibirá 60 euros por su colaboración.

No hay nada que indique o sugiera que algo extraño está pasando: el usuario sigue el enlace que le lleva a una página con un formulario de una encuesta de satisfacción al cliente, la lee y hace clic en el enlace. A continuación, aparece otro formulario, donde se informa al usuario de que lo único que tiene que hacer es escribir el número de su tarjeta de crédito, fecha de caducidad y el código *CVV* para poder recibir los 60 euros como se muestra en la *Figura 3.8*. Es evidente que en lugar de recibir el dinero en su cuenta, lo más probable es que los cibercriminales arrasen con sus fondos.

[9](19/septiembre/2011).http://www.techweek.es/seguridad/noticias/1009263004801/cibercriminales-utilizan-mcdonalds.1.html. Fecha de acceso noviembre del 2011

Figura 3.8 Página falsa para la encuesta de McDonalds

Curiosamente, la dirección en el campo "*De*" es: *mcdonalds@mcdonaldss.com*. Los expertos de *Kaspersky Lab*, recomiendan tener siempre en cuenta las "*s*" adicionales en el nombre del dominio ya que la creación de las direcciones que difieren de las auténticas por una sola letra es un truco muy común. Para burlar los filtros y listas negras, los cibercriminales recurren a sitios web infectados: el usuario sigue el enlace adjunto en el mensaje y lo primero que encuentra es una página web que sólo contiene unas líneas escritas en código *JavaScript*, el cual redirige al usuario al sitio principal de los ciberdelincuentes.

<script language=javascript>
*Top.location=”http://**.**.***.***./survey/”;*
</script>

Según los analistas de Kaspersky Lab hay que tener cuidado con este tipo de fraudes y no se deben seguir enlaces de mensajes de spam. Es aconsejable visitar siempre el sitio oficial de la empresa en cuestión, si se tienen dudas sobre la autenticidad de las ofertas, y contar con una buena solución antivirus actualizado.

3.1.10 Descubierta vulnerabilidad en sitio de American Express que permite Phishing.[10]

El especialista de seguridad Niklas Femerstrand ha descubierto una falla en el sitio Web de American Express que los atacantes pueden usar para robar, entre otras cosas, los datos de acceso a las tarjetas de crédito de los clientes. El hueco de Cross-Site Scripting (XSS) permite a los atacantes manipular ligas con el fin de escribir código JavaScript en el navegador de la víctima. El código es ejecutado en el contexto de la página Web de American Express. Los atacantes pueden leer las credenciales de acceso, robar cookies o inyectar software malicioso en el sistema víctima.

La vulnerabilidad se encuentra en una función de depuración a la que se puede acceder a través de Internet sin mayor protección, y es susceptible a Cross-Site Scripting. Los asociados de H en heise Security pudieron verificar la vulnerabilidad. Femerstrand dice que no fue capaz de ponerse en contacto con la empresa para reportar el problema, porque American Express no muestra detalles de contacto en su página para cuestiones de seguridad. Por lo tanto, decidió publicar los detalles completos acerca de la vulnerabilidad con la esperanza de que la compañía actúe.

La exposición de la falla, al parecer funcionó, y consiguió que la compañía de tarjetas de crédito reaccionara. American Express ha eliminado la página por ahora y, en un comunicado, dijo que la página no manejaba información de tarjetas de los clientes, tales como números de tarjeta o nombres; y precisó que la falla fue reportada porque permitía ataques de Phishing, no porque los datos se perdieran desde la página. La compañía también dijo que no tenía conocimiento de ninguna información que permita indicar que la falla fue utilizada para propósitos maliciosos. Sin embargo, no dijo si se estaba revisando los procesos para informar sobre problemas de seguridad.

[10](8/octubre/2011). http://www.tendenciadigital.com.ar/seguridad/noticias/descubierta-vulnerabilidad-en-sitio-de-american-express-que-permite-Phishing.html. Fecha de acceso noviembre del 2011

3.2- Informe de SPAM del primer trimestre de 2011

Los bancos Chase y Santander se convierten en destacados blancos de los *phishers*

- En el primer trimestre de 2011, el *Phishing* representó el 0,03% de todo el tráfico de correo.
- El *spam* probablemente superará el 80% del tráfico de correo el próximo trimestre si no se cierra alguna *red zombi*.
- La contribución de Asia y Latinoamérica al volumen total de *spam* a nivel mundial se ha incrementado, mientras que la de Europa se ha reducido. España es el país origen del 3,7% del *spam*.

Kaspersky Lab[11], líder en el desarrollo de sistemas de protección contra *software* malicioso, ataques de *hackers* y *spam*, presenta su Informe de *Spam* del Primer Trimestre de 2011. Durante este período y gracias a la campaña *anti-botnets* desarrollada durante el segundo semestre de 2010, el seguimiento de la evolución de *Spam* ha resultado especialmente interesante.

El volumen de *spam* en el tráfico de correo después de la clausura el año pasado de los centros de control de *redes zombis* aún no ha vuelto a sus niveles anteriores, aunque se ha incrementado llamativamente esto se puede apreciar más claramente con la grafica mostrada en la *Figura 3.9*.

Es casi seguro que en el próximo trimestre supere el 80%, si es que no se repite una intervención contra las *redes zombis* por parte de las autoridades.

[11] Kaspersky Lab (2011). *Kaspersky presenta informe de spam del primer trimestre del 2011*. http://www.kaspersky.com/sp/news?id=207732905. Fecha de acceso agosto del 2011

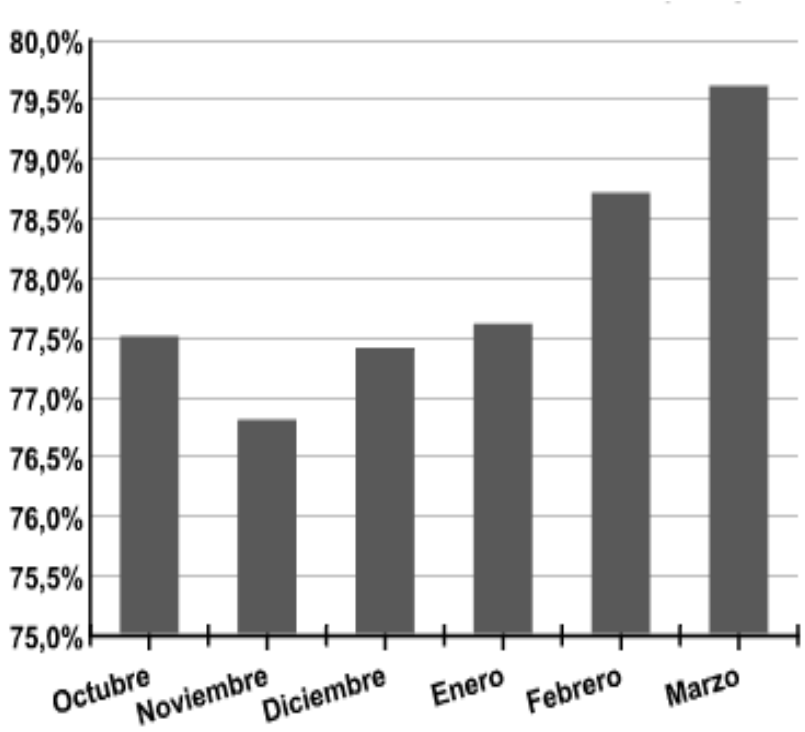


Figura 3.9 Spam en el tráfico de correo en el tercer trimestre de 2010 y en el primer trimestre de 2011

La clausura de los centros de control de la red *zombi Rustock* ha tenido un efecto en las estadísticas del primer trimestre de 2011, pero parece que los ciberdelincuentes ya estaban preparados para este evento o respondieron rápidamente a la situación, pues la recuperación fue rápida y la clausura de los centros de control no afectó seriamente el volumen total de spam. Respecto a los orígenes de spam, se han cumplido las previsiones de *Kaspersky Lab* sobre la relocalización de las redes zombis hacia regiones con débil legislación *antispam* y bajos niveles de competencia en tecnología informática.

La contribución de Asia y Latinoamérica al volumen total de spam a nivel mundial se ha incrementado, mientras que la de Europa se ha reducido. La *Figura 3.10* que demuestra claramente los sitios de donde ha surgido el spam en este primer trimestre del año.

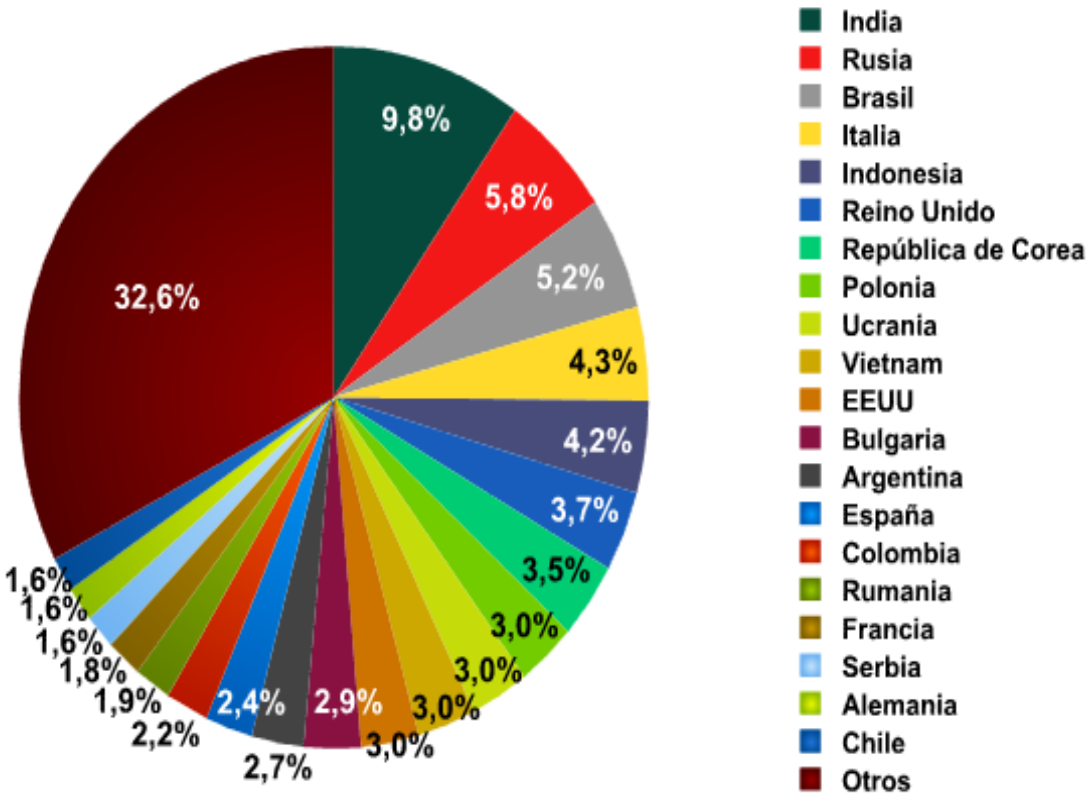


Figura 3.10 Orígenes de spam en el primer trimestre de 2011

El volumen de adjuntos maliciosos en el tráfico de correo sigue manteniéndose alto, al igual que el año pasado. La situación seguirá sin cambios hasta que nuevas *redes zombis* reemplacen a las que fueron clausuradas: la actividad spam ha sido criminalizada hace ya tiempo y resulta sorprendente que solo el año pasado comenzaran a aparecer grandes cantidades de programas maliciosos.

En el primer trimestre de 2011, los *spammers* prefirieron recurrir a técnicas ya probadas. Se distribuyó *spam* relacionado con videos y se intentó imitar los mensajes de los propios usuarios. El *spam* relacionado con videos no tuvo y no tendrá éxito mientras sigan siendo populares entre los *spammers* los falsos mensajes de usuario y la correspondencia personal. Es muy probable que seamos testigos de un cambio en las tácticas spam en el próximo trimestre.

El *Phishing* decrece. En el primer trimestre de 2011, el volumen de mensajes no deseados de tipo *Phishing* fue muy bajo y representó apenas el 0,03% de todo el tráfico de correo. Resulta interesante notar que el porcentaje de mensajes *Phishing* en el total del tráfico de correo se mantuvo sin cambios a través de todo el periodo. En los dos primeros meses se mantuvo en un 0,03%, mientras que en marzo decayó levemente, llegando al 0,02%. La *Figura 3.11* evidencia la disminución de *Phishing* en el mes de Marzo con respecto a Enero y Febrero, complementado con la Figura 3.12 la cual nos presenta las organizaciones más atacadas en el primer trimestre del 2011.

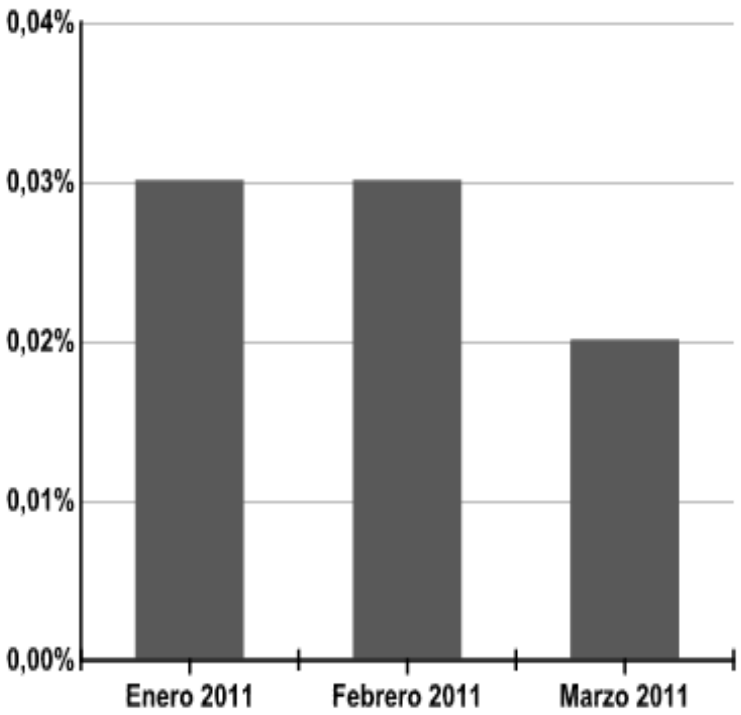


Figura 3.11 Porcentaje de mensajes Phishing en el tráfico de correo durante el primer trimestre de 2011

En el primer trimestre de 2011, PayPal y eBay mantuvieron su sólido liderazgo a nivel mundial entre las organizaciones atacadas con mayor frecuencia por los creadores de mensajes Phishing, o phishers, con respecto a los reportes recibidos en años pasados mientras que Facebook cayó al cuarto lugar y HSBC descendió al quinto.

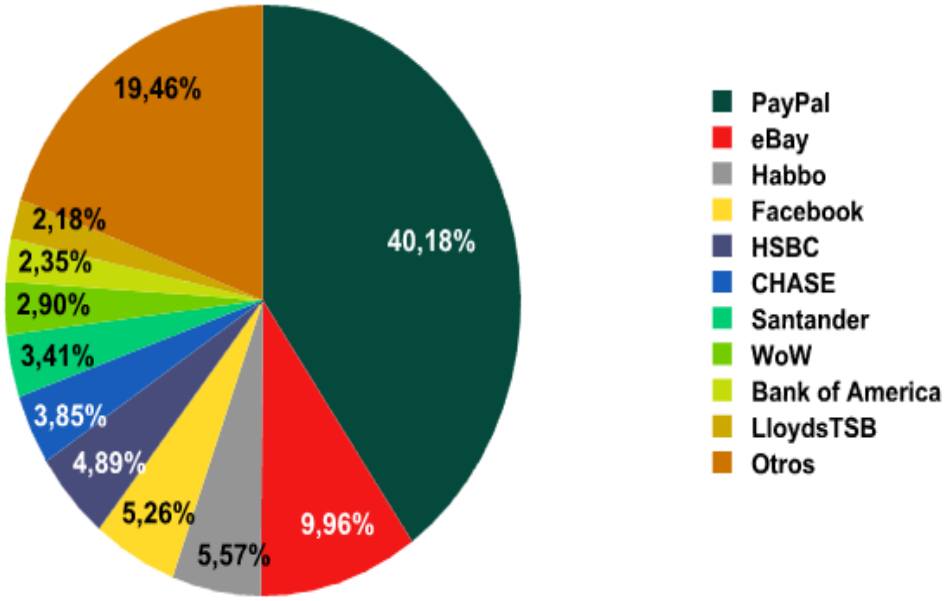


Figura 3.12 Top 10 de las organizaciones más atacadas por phishers en el primer trimestre de 2011

El sitio de la red social *Habbo* superó a *Facebook*, alcanzando el tercer lugar en cuanto a su popularidad entre los *spammers*. *World of Warcraft* solía ser un blanco preferido entre los *phishers*, pero cayó a la séptima posición en el primer trimestre de 2011, cediendo posiciones ante los bancos *Chase* y *Santande*r. Resulta llamativo que *Google*, que ocupaba la quinta posición a finales de 2010 con un 2,5%, ya no estuviera entre los Top 10 en el primer trimestre de 2011, puesto que los servicios como *Google AdWords* y *Google Checkout* sufrieron ataques menos frecuentes. Esta vez los *phishers* desviaron su atención hacia la muy popular red social brasileña *Orkut*, propiedad de Google. Los ataques a esta red social alcanzaron el 1,96% del total, colocándola en la duodécima posición de la lista de organizaciones preferidas por los ataques de los *phishers*.

3.3- Indicadores

Como se puede apreciar en las estadísticas de incidencia de esta organización, los bancos son los blancos preferidos para el Phishing así como se mostró en nuestro análisis previo de las noticias recolectadas en el mismo tiempo y aun más recientes, de esta forma queda comprobada que la tendencia de este tipo de ataques que ejecutan los ingenieros sociales es suplantar páginas que utilizan usualmente usuarios inexpertos en el tema, ya que lo único que se necesita es que la página parezca oficial.

De la misma forma las redes sociales tienen la misma problemática la falsificación de su página de acceso, esto es muy común, debido a que es una forma fácil de apoderarse de los datos personales de sus usuarios para posteriormente venderlos o a partir de ellos poder enviar correo basura a sus contactos. Las páginas como *Paypal* son los blancos predilectos, debido a que una vez obtenida la información puede ser transferida fácilmente a una cuenta particular, de igual forma se pueden conseguir objetos varios con la cuenta de otra persona.

3.4 Análisis de SYMANTEC septiembre 2011

En septiembre, la actividad de *Phishing* e correos electrónicos disminuyo 0.26% desde agosto 2011, uno de cada 447.9 correos electrónicos contiene algún tipo de ataque de Phishing. Con ayuda de la *Figura 3.13* se observara la tasa de *Phishing* a nivel mundial así como su compartimiento.

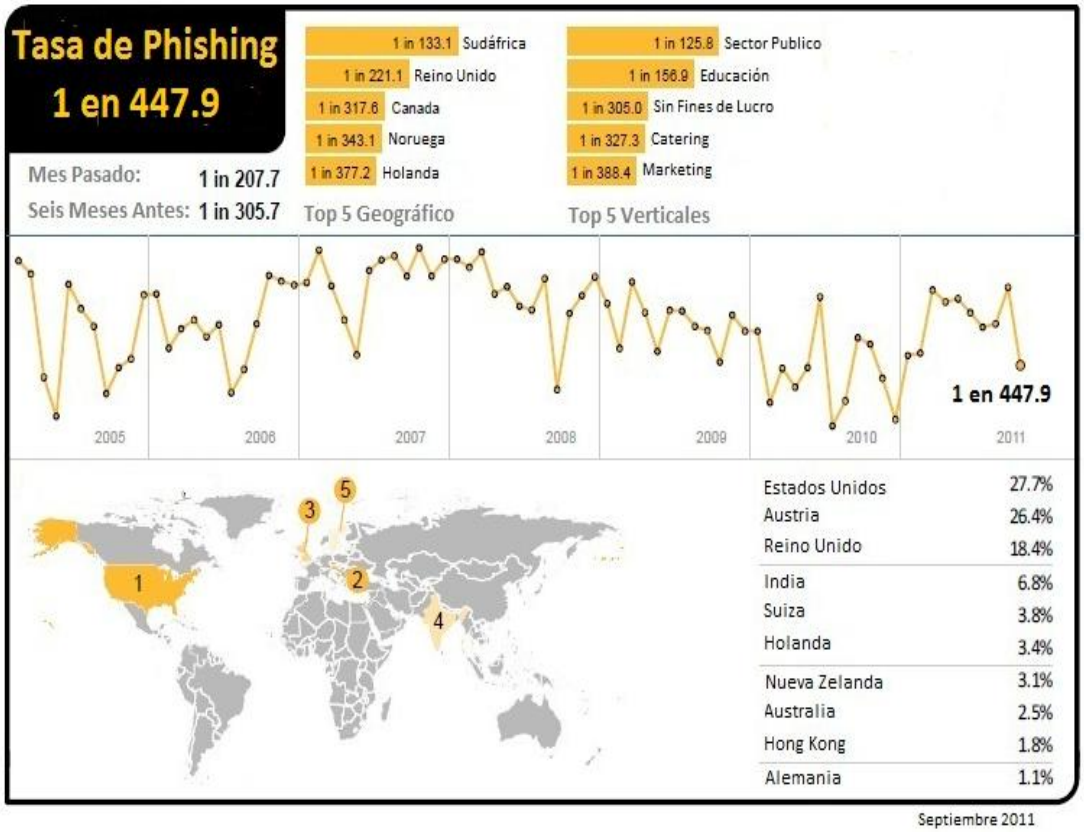


Figura 3.13 Tasa de Phishing

Los ataques de *Phishing* en el Sur África han ido han aumentado una vez más haciéndolo el objetivo número uno geográficamente para los ataques de *Phishing*, con uno en 133.1 correos identificados como *Phishing*. El Reino Unido siguió siendo el segundo objetivo para los ataques de *Phishing* con uno en 221,1 correos electrónicos identificados.

Los niveles de *Phishing* para Estados Unidos eran de uno en 985.6 y uno en 317.6 para Canadá. En Alemania los niveles de Phishing eran de uno en 1,125, uno en 1,071 en Dinamarca y uno en 377,2 en Holanda. En Australia la actividad *de Phishing* fue de uno en 740 correos y uno en 1,882 en Hong Kong; para Japón era uno en 12,812 y uno en 1,958 para Singapur. En Brasil uno en 439 correos se bloqueó como *Phishing*.

El sector Público sigue siendo el objetivo principal para la actividad del *Phishing* en el mes de septiembre, con uno en 125,8 correos que comprometen un ataque de *Phishing*. Los niveles de Phishing para el sector Químico y Farmacéutico alcanzo uno en 797,3 y uno en 754,6 respectivamente, para el sector de Servicios uno en 664,5, uno en 156,9 para la el sector Educativo y uno en 388,6 para el sector Financiero.

3.4.1- Análisis del Phishing en sitios Web.

El numero de sitios *Web* con *Phishing* ha disminuido 12.2% en septiembre. El numero de sitios *Web* creados por kits de herramientas automatizadas ha disminuido aproximadamente un 38.6%. El numero de direcciones *URLs* de *Phishing* ha disminuido un 2.6% y las sitios *Web de Phishing* usando las direcciones IP en lugar de los nombres de dominio disminuyó en un 16.9%.

El uso de servicios de *hosting* en *Web*s legítimos para servicios de *Phishing* representa aproximadamente el 6% de todos los sitios *Web de Phishing*, disminuyo un 32.7% de los meses anteriores.

El numero sitios de *Phishing* que no está en ingles registro una disminución del 14.1%. Los sitios más comunes que no están en ingles para la práctica del *Phishing* son Portugués, Francés, Italiano y Español. La siguiente *Figura 3.14* muestra con claridad la localización de las zonas con nivel más alto de *Phishing*, posteriormente la *Figura 3.15* nos revela los resultados de las tácticas más usadas y al final podemos apreciar que organizaciones de la industria son más atacadas con ayuda de la *Figura 3.16*.

País	Septiembre	Agosto
Estados Unidos	50.4%	49.8%
Alemania	6.2%	6.5%
Reino Unido	3.8%	3.8%
Canada	3.1%	3.7%
Rusia	3.0%	3.0%
China	2.7%	2.5%
Francia	2.6%	2.7%
Brasil	2.5%	2.6%
Holanda	2.3%	2.3%
España	1.5%	<0.5%

Figura 3.14 Mapa con la localización geográfica de las zonas con más nivel de Phishing

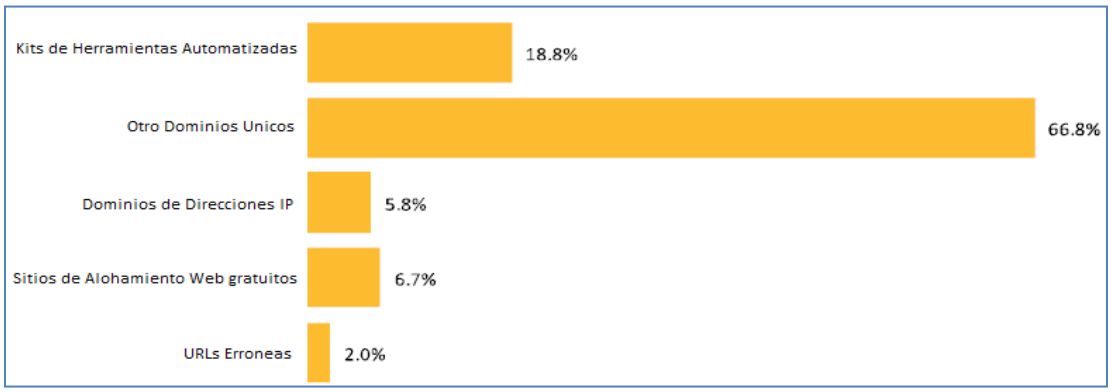


Figura 3.15 Resultados de la distribución de las tácticas de Phishing

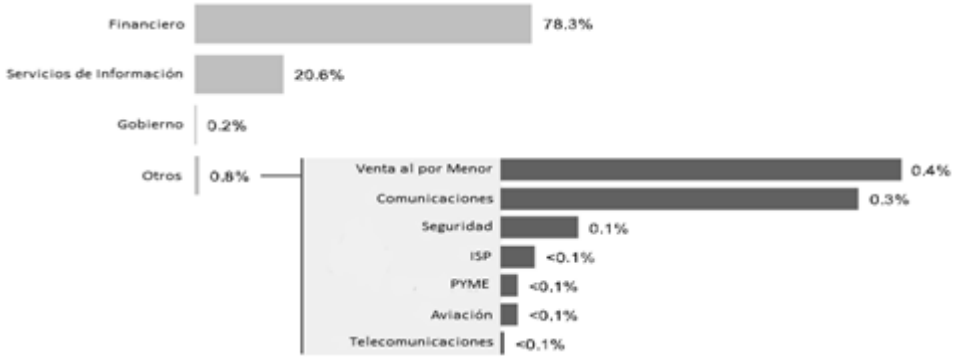


Figura 3.16 Resultado de los ataques de Phishing a organizaciones, en el sector industrial

3.5 Tendencias

Después de revisar las noticias anteriores revelamos que la tendencia a seguir por los ingenieros sociales que usan el *Phishing* para sus estafas es el enviar correos fraudulentos a los usuarios, para que estos loguen a una página falsa y poder sustraer así la información personal que desean. Para esto lo más usado comúnmente son paginas de bancos o servicios tipo *PayPal*, donde se maneja dinero, de la misma forma esta práctica se presenta continuamente en redes sociales importantes en la actualidad como son *Facebook y Twitter*. En la Figura 3.17 se puede observar las tendencias que sigue los ingenieros sociales para sus ataques elaborada a partir de la *Tabla 3.1*.

En menos frecuencia encontramos que los ingenieros sociales utilizan otras técnicas de *Phishing* como son:

- Explotar vulnerabilidad de sitios *web*.
- Aplicaciones falsas para dispositivos móviles.
- *VoIP*, específicamente en el uso de *skype*.

A continuación se presenta una tabla mostrando la tendencia descrita anteriormente.

Tabla 3.1 Tendencias del Phishing

Noticia	Numero de incidencias
Suplantación de Pagina Web (Portales de Bancos, Twitter, etc.)	7
Vulnerabilidades de Sitios	1
VOIP	1
Aplicaciones Falsas	1

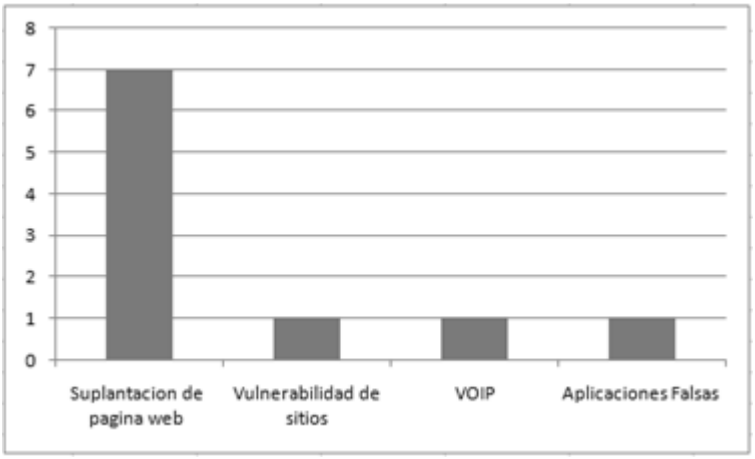


Figura 3.17 Tendencia obtenida de las noticias analizadas

Ahora comparando los resultados obtenidos con el número de incidencia de organizaciones experimentadas en el tema.

CAPÍTULO IV

TECNOLOGÍA APROPIADA PARA LA SEGURIDAD

En este capítulo se habla sobre las diferentes tecnologías disponibles para solucionar el problema de seguridad, tanto para las empresas como para los usuarios.

CAPÍTULO IV TECNOLOGÍA APROPIADA PARA LA SEGURIDAD

4.1- Recomendaciones para prácticas de seguridad dentro de empresas

- *Emplear estrategias intensas de seguridad*. Se debe enfocar la defensa en más de una estrategia de seguridad y buscar que estás se apoyen mutuamente para proteger el sistema de cualquier simple fallo. Entre algunas acciones que se debe hacer es la actualización continua de servidores, así como el programa antivirus, detectores de intrusos y herramientas de seguridad relacionadas al control de la red.

- *Estar al tanto sobre nuevas amenazas de red además de tener un control sobre el tráfico de red.* Se debe monitorear y registrar los intentos de intrusión así como el tráfico sospechoso en la red, identificar los intentos de conexión de hosts sospechosos. Recibir y estar atentos a nuevas alertas de vulnerabilidades y amenazas de distintas empresas para llevar a cabo acciones preventivas.

- *Tener sólo un antivirus no es suficiente*. Un *antivirus* no es suficiente para proteger completamente contra las nuevas amenazas y ataques en la red. Se debe usar un buen criterio de valoración para escoger e implementar paquetería de seguridad que ofrezcan protección contra:

    - Vulnerabilidades que existan en él sistema y que puedan ser explotadas en un futuro, que proteja contra ataques de Ingeniería Social y que detenga *malware* sin que este pueda llegar al equipo final.
    - Protección contra ataques repentinos (ataques de día cero).
    - Que considere la detección *malware* basado en la nube para proporcionar una protección proactiva en contra de amenazas.
    - Registros que muestren un criterio de riesgo-reputación de cualquier aplicación.
    - Capacidad de análisis automático de comportamiento de *malware*.
    - Control para evitar que aplicaciones y *plug-ins* con contenido malicioso se descarguen o se ejecuten automáticamente.
    - Control de dispositivos USB.

- *Utilizar Sistemas de Prevención de Pérdidas de Datos*. Implementar un Sistema de Prevención de Pérdidas de Datos que pueda identificar donde reside la información sensible, controle su uso y lo proteja a esta información de perdidas. El Sistema de Prevención de Pérdidas de Datos debe tener la facultad de controlar el flujo de datos y controlar los datos que salgan fuera de la organización, además los Sistemas de Prevención de Pérdidas de Datos deben ser configurados para identificar y bloquear copias o descargas de datos sensibles.

- *Utilizar técnicas confiables de encriptación para proteger datos sensibles*. Elaborar, aplicar y hacer cumplir políticas de seguridad con respecto al almacenamiento, uso y protección de datos sensibles encriptados. El acceso a estos datos debe ser restringido y con un fuerte sistema de control de acceso. Además, se debe implementar un Sistema de Prevención de Pérdidas de Datos, que nos permitirá identificar, monitorear y proteger datos, además de que nos ayudará para mitigar el posible daño causado por fuga o pérdida de información.

- *Actualizar constantemente las medidas de seguridad.* Con millones de variantes de *malware* detectadas, sumados a los miles que nacen día tras día, las empresas deben actualizar sus sistemas de seguridad contra virus por lo menos una vez al día, si no es que varias veces al día si es posible.

- *Crear, aplicar y hacer cumplir políticas de seguridad acerca de medios extraíbles.* Siempre que sea posible, se debe limitar el uso de dispositivos de almacenamiento externos, tales como discos duros y otros medios extraíbles como memorias flash, tarjetas de memoria, etc. Estos dispositivos pueden introducir programas maliciosos, así como facilitar el robo de información sensible. Si el uso de dispositivos externos está permitido dentro de las políticas de seguridad, antes de permitir su uso se deben analizar en busca de virus y utilizar el Sistema de Prevención de Pérdidas de Datos para monitorear las acciones que se realicen y restringir la copia de datos confidenciales.

- *Realizar actualizaciones y depuraciones*. Realizar la actualización, revisión y depuración de aplicaciones y navegadores obsoletos e inseguros, así como obtener los últimos complementos para las versiones finales disponibles.

- *Aplicar una política eficiente de contraseñas.* Asegúrese de que las contraseñas sean fuertes, que contengan por lo menos de 8 a 10 caracteres de longitud y que incluyen una mezcla de letras y caracteres alfa-numéricos. Animar a los usuarios para que eviten reutilizar las mismas contraseñas en diferentes sitios web y prohibir el intercambio de contraseñas. Las contraseñas deben cambiarse regularmente, al menos cada 90 días. Evite escribir las contraseñas.

- *Restringir el correo electrónico con archivos adjuntos*. Configure los servidores de correo electrónico para bloquear o eliminar mensajes que contengan archivos adjuntos los cuales son utilizados comúnmente para propagar virus, en especial archivos *.VBS, .BAT, .EXE, .PIF, y .SCR.* además se deben analizar los archivos de documentos que puedan venir adjuntos a un correo electrónico *como .DOC, .PDF, .DOCX*, etc. antes de ejecutarse.

- *Asegúrese de que se tengan planeados procedimientos de respuesta a infecciones e incidentes.*

    - Asegúrese de que se tenga a la mano información de contactos de los proveedores de seguridad.
    - Asegurar que él respaldo está en funcionamiento, esto con el fin de restaurar los datos perdidos o comprometidos en el caso de un ataque exitoso o pérdida de datos catastrófica.
    - Hacer uso de las capacidades de detección de infección de la puerta de entrada, servidores, *firewalls* y terminales para identificar cuáles son los sistemas infectados.
    - Aislar los equipos infectados para evitar el riesgo de infección aún más dentro de la organización.
    - Si los servicios de red son explotados por código malicioso, o alguna otra amenaza, deshabilite o bloquee el acceso a los servicios hasta que se solucione el problema.
    - Realizar un análisis forense en los equipos infectados y restaurar equipos si es posible.

- *Educar a los usuarios entorno a las nuevas amenazas.*

  - No abra archivos adjuntos a menos que se sepa el contenido de ellos y que vienen de una fuente conocida y de confianza, no ejecute el *software* que se descarga desde Internet a menos la descarga haya sido escaneada.
  - Tenga cuidado al hacer clic en las direcciones *URL* en los correos electrónicos o en redes sociales, incluso cuando provengan de fuentes de confianza y amigos.
  - No haga clic en atajos de *URL* sin obtener una vista previa con ayuda de las herramientas disponibles y complementos.
  - Recomiende a los usuarios tener cuidado con la información que proporcionan dentro de las redes sociales (si es posible evite que los usuarios tengan acceso a estas páginas) que podría ser utilizada para realizar un ataque.
  - No se fíe de los motores de búsqueda.
  - Sólo descargue el *software* (si se permite) directamente desde el portal de los proveedores.
  - Si los usuarios ven una advertencia que indica un posible ataque o infección después de hacer clic en una *URL* o mediante una búsqueda los usuarios deben cerrar o salir del navegador utilizando *Alt-F4* o el administrador de tareas.

4.2- Recomendaciones para prácticas de seguridad para usuarios y consumidores

- *Proteja su equipo*: Use una solución de seguridad de Internet que incluya las siguientes características para una máxima protección contra códigos maliciosos y otras amenazas:

  - Un antivirus que impida que el malware se pueda ejecutar.
  - Un *firewall bidireccional* bloqueará malware protegiendo aplicaciones y servicios vulnerables que estén corriendo en la computadora.
  - Que brinda protección contra kits de herramientas maliciosas y ataques de Ingeniería Social.

- *Manténgase al día*. Mantenga el antivirus actualizado, actualizar por lo menos una vez al día, teniendo las firmas de virus más recientes, usted puede proteger su equipo contra los últimos virus y *malware*. Mantenga actualizado su sistema operativo y sus navegadores de Internet.

- *Se consiente de las amenazas de seguridad*. Tenga en cuenta que existe malware que es instalado automáticamente al instalar alguna otra aplicación o al consultar algún archivo adjunto o haciendo click en el link de alguna pagina web:

    - Al descargar versiones *piratas* o *crackeadas* de *software* es probable que además se descargue malware que puede infectar el equipo o por otra parte tratan de aparentar una supuesta infección, pidiendo una suma de dinero para eliminarla.
    - Tenga cuidado con los sitios de internet que visite. El *malware* se puede propagar fácilmente en sitios poco confiables como sitios de pornografía, apuestas y páginas de descarga de *software* pirata.
    - Lea los tratados de licencia con cuidado y entendía todos los términos antes de acceder.

- *Aplicar una política eficiente de contraseñas.* Asegúrese de que sus contraseñas sean una combinación de letras y caracteres alfanuméricos con longitud entre 8 y 10 caracteres. Palabras comunes no deben usarse como contraseñas. No use las mismas contraseñas para distintos sitios web.

- *Piensa antes de dar click*. Nunca veas, abras o ejecutes ningún, correo con archivos adjuntos sin conocer quién es el remitente. Incluso no hay que estar totalmente confiado aun si se sabe quién es el remitente:

    - Sea cuidadoso cuando haga clic en *URL's* que aparecen en correos, programas y redes sociales incluso cuando el remitente es gente conocida.
    - No haga clic en atajos de URL sin obtener una vista previa con ayuda de las herramientas disponibles y complementos.

- Tenga cuidado de los anuncios que aparecen en las ventanas emergentes preguntado si desea instalar algún tipo de aplicación. Solo descargue programas de las páginas oficiales de sus desarrolladores.

- *Cuide sus datos personales*. Limite la cantidad de información personal que pública en internet (en especial en las redes sociales) por lo general esta información es recolectada y usada para actividades maliciosas.

  - Nunca de información confidencial o financiera a menos que éste totalmente seguro que el que pide la información sea legítimo.
  - Revise su banco, tarjeta de crédito e información crediticia en busca de alguna actividad irregular. Evite las compras por Internet desde computadoras con acceso público (como café internet, bibliotecas, etc.) o utilizando redes *Wi-Fi* sin seguridad.
  - Si se conecta a través de una red *Wi-Fi*, utilice *HTTPS* cuando cheque su correo electrónico o su perfil de las redes sociales.

- *Comparta su dirección de correo electrónico sólo con fuentes confiables*. Sólo su familia, amigos y contactos comerciales de confianza deberían tener su dirección de correo electrónico personal. No publique su dirección de correo electrónico en sitios Web, foros o salas de chat. Si publica su dirección de correo electrónico, estará vulnerable para recibir *spam* o se podrá entregar su dirección a otros. Si desea subscribirse a un boletín o sitio Web y recibir un correo electrónico de confirmación para transacciones en línea, considere usar una dirección de correo electrónica genérica que no contenga información personal.

- *Utilice los programas de Mensajería Instantánea con precaución*. Si utiliza programas de mensajería instantánea para comunicarse con sus amigos y familiares, evite enviar información personal. Nunca use su nombre real ni acepte a extraños en sus grupos.

- *Cree una cuenta de correo electrónico compleja*. Con una cuenta de correo electrónico compleja, se hace más difícil para los *hackers* autogenerar su correo electrónico, enviar correo electrónico spam u otros tipos de ataques a su correo electrónico. Intente utilizar caracteres alfanuméricos en una combinación única. Substituya los números por letras cuando pueda.

- *Nunca escriba información personal en una ventana emergente.* A veces aparecen ventanas emergentes no autorizada creada por el estafador en páginas licitas, con espacios en blanco para que escriba su información personal. Si la llena, su información se enviará al estafador. Instale un software con bloqueo de ventanas emergentes para ayudarle a evitar este tipo de ataque fraudulento**.**

4.3- Recomendaciones para prácticas de seguridad con el uso de dispositivos móviles.

Si bien los casos de ataques a dispositivos móviles eran muy pocos, los últimos años se ha visto un aumento considerable en ilícitos relacionados con estos dispositivos los factores que contribuyeron el crecimiento de estos ataques son:

- Es relativamente barato conseguir un teléfono inteligente para acceder a internet.
- La mayoría de la gente que usa internet en dispositivos móviles desconocen las técnicas de los *hacker* para obtener información.
- Muchos usuarios de internet sólo usan los dispositivos móviles para actualizar su perfil en las redes sociales.
- Aumento en la cantidad de troyanos para móviles que al ejecutarse causan daños.
- Es donde hay más posibilidades de ataque por parte de los *hackers*, por el solo hecho de que las redes sociales reciben millones de visitas al día y los dispositivos móviles son cada vez más populares.
- Todos los días hay nuevos usuarios de internet que nunca habían usado internet y ahora lo hacen por primera vez, esa clase de usuarios son un blanco fácil de los hackers.

- *Nunca almacene datos personales sensibles en sus dispositivos móviles.* Dado a que es muy fácil extraviar este tipo de dispositivos, nunca se debe almacenar datos que puedan ser utilizados para fraudes por terceras personas como información bancaria.

- *No instale aplicaciones de sitios apócrifos*. Dado que la industria de seguridad en dispositivos móviles no esta tan desarrollada como su contraparte en computadoras personales, el usuario debe tener cuidado de las aplicaciones que descarga e instala ya que estas pueden contener algún tipo de malware móvil, solo descargue aplicaciones legales a través de los portales de la compañía.

- *No utilice la opción de almacenar contraseñas.* En el caso de pérdida, al dejar activado el auto inicio de sesión es igual a dejar abierta la oportunidad de sufrir algún tipo de fraude como el robo de identidad o fraudes bancarios.

- *Actualice su equipo.* Actualizar su dispositivo móvil es la mejor manera de proteger contra vulnerabilidades o contra posibles ataques de *malware*.

- *Mantenga el bluetooth apagado.* Si no está utilizando el bluetooth debe tenerlo en modo inactivo. El *bluetooth* es un servicio, que debido a sus vulnerabilidades, es usado para cometer fraudes como el robo de información o también existen aplicaciones que permiten enviar c*omandos AT* para poder realizar llamadas o enviar mensajes desde el dispositivo atacado.

- *No ingrese información confidencial cuando use redes sin protección.* Si está utilizando una red pública como la que se encuentra en parques o centros comerciales o redes sin protección, evite acceder a portales bancarios o sitios que pueda contener información sensible.

- *Aplicar una política eficiente de contraseñas.* Asegúrese de que sus contraseñas sean una combinación de letras y caracteres alfanuméricos con longitud entre 8 y 10 caracteres. Palabras comunes no deben usarse como contraseñas. No use las mismas contraseñas para distintos sitios web.

4.4- Tecnologías para la protección de Phishing y otras amenazas

- *Antivirus basado en la nube:* Los antivirus son las herramientas más utilizadas para detectar y detener archivos maliciosos, sin embargo los antivirus convencionales fallan al no poder detectar muchas de las amenazas modernas y su creciente complejidad ha dado lugar a vulnerabilidades que están siendo explotadas por *malwares*. Estas limitaciones llevaron a diseñar un nuevo modelo para la detección de *malware*. Con esta idea surgen los antivirus basados en la nube, que básicamente realizan todas las funciones de los antivirus convencionales con la gran diferencia que el programa realiza todas las funciones desde la nube permitiendo no sólo que no se ocupe espacio en disco duro si no que la rapidez de ejecución se realice de una manera mucho más rápida, esto gracias a que el *software* almacena los resultados de análisis posteriores para no tener que repetir dos veces la misma operación. Un archivo ejecutable se aloja en la memoria caché para indicar qué se ha revisado ya y que está limpio.

  La clave está en que el proceso de detección se realiza a través de la nube virtual, lo que permite ejecutar varios antivirus de forma simultánea y aumenta las garantías de desinfección, sin problema de compatibilidades entre sistemas.

  Aunque suene como un excelente método para la detección de *malware* hay que considerar las desventajas siendo la más notoria que estas herramientas necesitan de conexión permanente a internet, si no se puede acceder a internet o el *malware* no permite una conexión nuestro equipo quedaría totalmente vulnerable. Otro punto a considerar es que estamos enviando información al servidor de la empresa, lo que puede ocasionar que se vea comprometida. Este proyecto conocido como *CloudAV* nació en la universidad de Michigan EEUU, la idea principal era tener un antivirus situado en internet de tal forma que cualquiera pueda acceder a él.
  El primer antivirus de este tipo lanzado comercialmente es el Panda Cloud Antivirus por la compañía Panda Security disponible en 11 idiomas, Panda Cloud Antivirus funciona bajo los sistemas operativos Windows XP (32 bits), Windows Vista (32 bits y 64 bits) y Windows 7 (32 bits y 64 bits), ocupando tan solo 100MB de disco duro para su instalación y 64 MB de RAM. En la *Figura 4.1* podemos ver la pantalla de Panda Security después de haber realizado un chequeo.

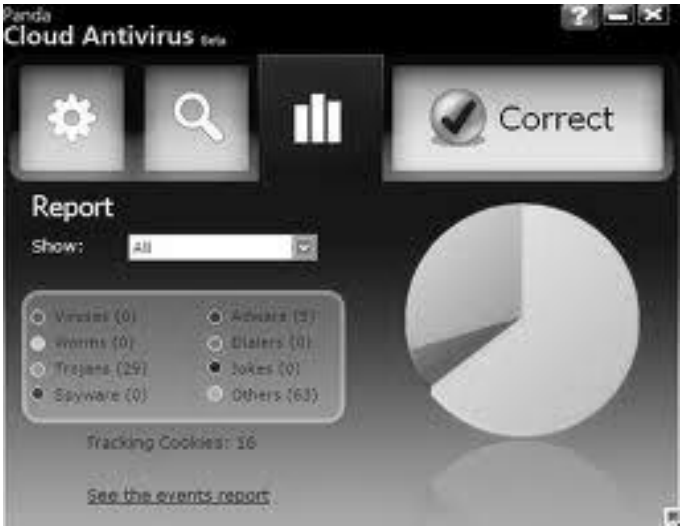


Figura 4.1 Panda Cloud Antivirus

- *Antivirus con análisis de comportamiento de malware.* Los antivirus típicos tienen que haber identificado y visto una amenaza antes de poder proporcionar una protección adecuada frente a ella, entonces se ofrece la protección a través de una actualización de firmas o huellas, que debe ser redactada por un investigador de antivirus. Esto supone un largo espacio de tiempo en el que no se detectan amenazas y, por tanto, pueden infectar su equipo incluso aunque tenga un programa antivirus instalado. Bajo la problemática de que los malware se actualizan con mayor velocidad que las bases de datos de los antivirus, surgen los antivirus con capacidad de análisis de comportamiento de *malware*, estos indagan en las distintas características y comportamientos que posee el *software* para poder identificar si se trata de malware o una aplicación segura. En este sentido, todas las compras, así como los envíos y transferencias que impliquen un tráfico dinerario deben estar protegidas no sólo por los tradicionales antivirus y antispyware, sino también por complementos como estos que funcionan como un verdadero escudo para salvaguardar información de importancia para todos los usuarios.

- *Herramientas para el control de dispositivos USB.* Una de los principales formas de robo de información e la infección del equipo es el puerto USB es por eso necesario tener un control de este puerto sobre todo si se cuenta con información sensible que puede ser sustraída, existen dos tipos de programas para el control del puerto USB, el primer tipo nos sirve para llevar el registro de la actividad en los puertos USB como las características físicas del dispositivo conectado, los protocolos que se utilizan y analiza el estado de los puertos. El otro tipo nos permite llevar un registro de dispositivos y permite elegir cuál de ellos está autorizado, bloqueando cualquier dispositivo que no lo esté. En la *Figura 4.2* se observa el control de la USB que podemos tener mediante el registro de las actividades y en la *Figura 4.3* el control mediante los dispositivos autorizados.

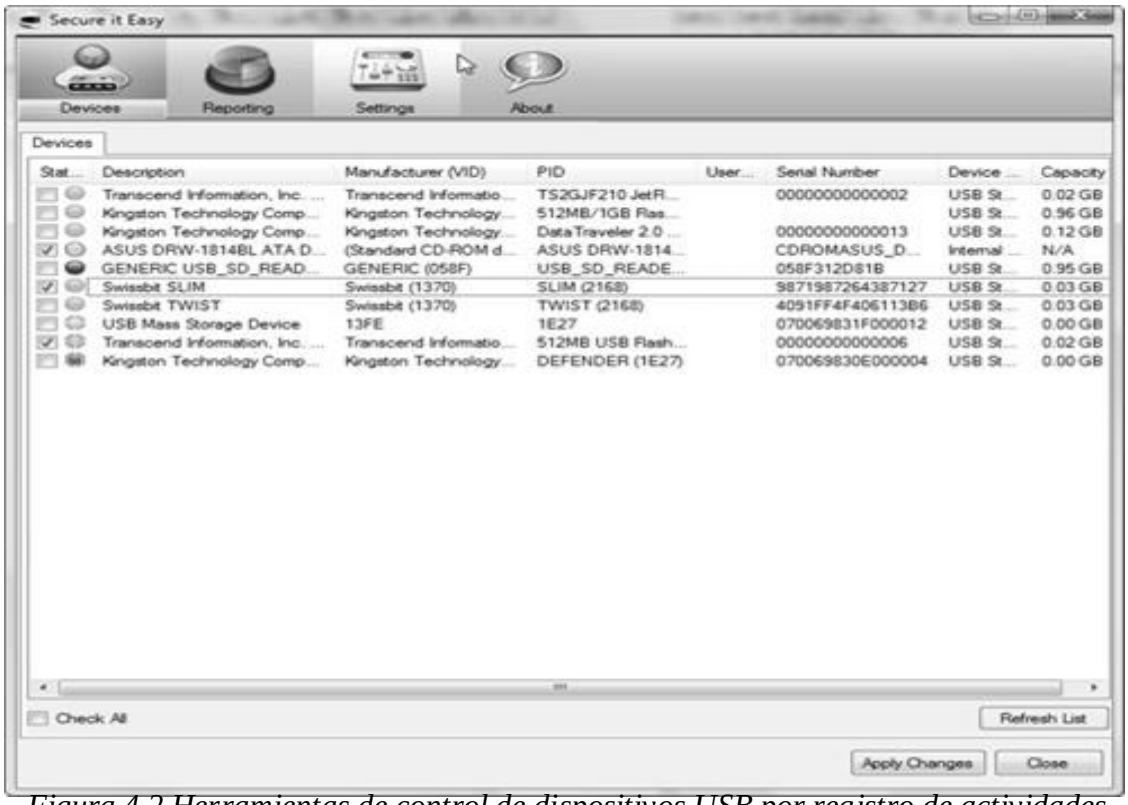


Figura 4.2 Herramientas de control de dispositivos USB por registro de actividades

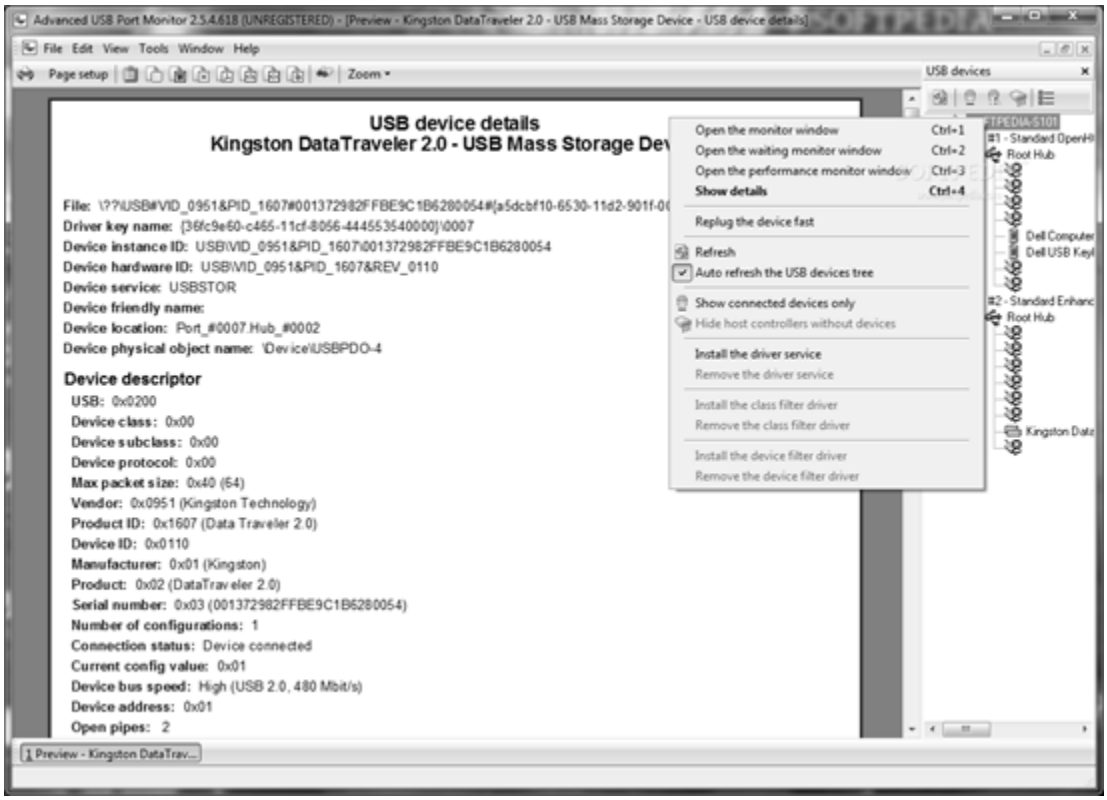


Figura 4.3 Herramientas de control de dispositivos USB por dispositivos autorizados

- *Software de prevención de pérdidas de datos.* La prevención de pérdida de datos (*DLP*, por sus siglas en inglés) es el proceso para detectar y prevenir el robo o la divulgación no autorizada de información sensible tanto de los datos en uso (como información en las terminales), datos en movimiento (datos transmitidos por red) y datos en reposó (datos almacenados). La *DLP* consiste en la combinación de personas, procesos y tecnología que trabajan conjuntamente para ayudar a garantizar que los datos se utilicen de la manera deseada. Las organizaciones no pueden correr el riesgo de sufrir consecuencias perjudiciales debidas a la pérdida de datos o sanciones por infringir las normas es por eso que es fundamental la implementación de este sistema. Existen 5 tipos de sistemas de *DLP* dependiendo de la necesidad que se requiera cubrir:

- *DLP de red:* este sistema se instala en los puntos de salida de la red, analiza el tráfico de red en busca de datos sensibles que se pudieran estarse enviando en forma ilícita.
- *DLP de almacenamiento.* Este sistema se instala en los puntos de almacenamiento para descubrir si cierta información se está almacenando en lugares inapropiados o sin garantías de seguridad.
- *DLP de equipos terminales.* Estos sistemas se ejecutan en las estaciones de trabajo de los usuarios finales o los servidores de la organización, se puede utilizar para controlar el flujo de información entre los grupos o tipos de usuarios. También puede controlar las comunicaciones de correo electrónico y mensajería instantánea antes de que se almacene. Estos sistemas tienen la ventaja de que pueden monitorear y controlar el acceso a los dispositivos físicos (como dispositivos de almacenamiento de datos). Algunos sistemas, también puede proporcionar los controles de aplicación para bloquear el intento de transmisiones de información confidencial, y proporcionar una respuesta inmediata al usuario. Tienen el inconveniente de que necesita ser instalado en cada estación de trabajo en la red y no puede ser utilizado en dispositivos móviles (por ejemplo, teléfonos móviles y PDA).
- *Identificación de Datos.* Los sistemas *DLP* incluyen una serie de técnicas para la identificación de información confidencial o sensible, para esto utilizan varios métodos de análisis profundo del contenido, que van desde palabras clave, diccionarios, y expresiones regulares.
- *Detección de Fugas.* En caso de existir una fuga de información, este sistema se encarga de encontrar el medio y la forma de cómo se llevo a cabo esta fuga.

- *Antivirus para dispositivos móviles.* Si bien hace algunos años eran muy escasos los casos de virus en dispositivos móviles, el riesgo de adquirir uno de esos virus aumento junto a las capacidades de conexión de los dispositivos móviles. Primeramente la seguridad en estos dispositivos estaba orientada a la pérdida del equipo y la protección de sus datos, con las apariciones de las primeras aplicaciones maliciosas la seguridad se orientaba a evitar que los archivos se infectaran, hoy en día a todo lo anterior se suma que las aplicaciones maliciosas en los mercados de aplicaciones están en aumento y la necesidad de proteger sus datos ante ataques cibernéticos. Debido a sus características los virus que van dirigidos a las computadoras personales generalmente no pueden infectar a un dispositivo móvil, pero también hay que tener en cuenta que hoy en día muy pocos dispositivos móviles cuentan con una protección antivirus. Al igual que en las computadoras, los malware pueden llegar a estos dispositivos por distintas formas, ya sea por vía online o por memorias flash infectadas. Los peligros acechan en la red y los tipos de malware dependen en gran parte del tipo de sistema operativo que usan. El comportamiento del malware puede variar dependiendo con que objetivos fue diseñado, puede dirigirse al acceso remoto no autorizado de una dispositivo infectado para: realizar ataques de suplantación de *DNS* que redirigen sin que se dé cuenta el usuario a sitios maliciosos, al robo de información confidencial de carácter financiero, como son los *logins* de usuarios, *pins* y contraseñas, ataques de *Phishing*, etc. Muchos de los programas maliciosos que atacan al sistema operativo *Android* son clones casi idénticos de las aplicaciones legítimas y generalmente los usuarios confían en estas y la descargan. Un antivirus para dispositivo móvil es un medio de detección y protección para identificar y eliminar virus en dispositivos móviles, entre sus principales funciones que realiza es el análisis antivirus en tiempo real de todos los mensajes y conexiones entrantes, análisis antivirus sin perjudicar la memoria del dispositivo, protección *antispam*, protección contra mensajes *SMS* no deseados. filtrado según remitentes y contenidos, etc. En la *Figura 4.4* podemos ver un antivirus para dispositivos móviles así como sus funciones.

Figura 4.4 Antivirus móvil

4.5- Protección para el navegador Web

En la actualidad tenemos diversas herramientas que nos permite: evitar páginas fraudulentas, bloquear la publicidad, tener información sobre las páginas que visitas, etc. Es muy útil tener estos complementos de esta forma se tendrá una protección más completa de nuestras búsquedas o navegación en internet. Algunos ejemplos de las ventajas de usar estos complementos son: compras en páginas web del extranjero ya que te indica: el país en donde se encuentra la página, su fecha de creación, etc. Permiten luchar contra el *Phishing*.

A continuación observaremos algunos complementos de protección para los navegadores.

- *Dr.Web para Firefox*. De la gran variedad de complementos que existen para *Firefox* hay uno que nos puede ser de mucha utilidad para proteger nuestro PC. Este complemento funciona como un escáner bajo demanda y no consume nada de recursos, no se trata de un antivirus que se instala en el PC, sino que se instala únicamente en el navegador *Firefox*.

Dr.Web es un antivirus bastante especial sobre todo por su sorprendente base de datos y su fina detección de virus por lo general desconocidos para otros. Para utilizarlo primero debe de instalarse en los complementos de *Firefox*, posteriormente después de instalarse y reiniciar se hace click derecho sobre un enlace de descarga y veras aparecer una nueva función en el menú contextual, para analizar el enlace de descarga se debe de seleccionar la opción *"Scan with Dr.Web"* Si se trata de un archivo infectado te aparecerá un mensaje informando que se ha detectado y bloqueado la infección. Como podemos ver, si no contáramos con este complemento, de seguro bajaríamos el archivo e infectaríamos la PC.

- *Netcraft Toolbar*. Es una aplicación gratuita para *Windows* que instala una barra en tu navegador *Internet Explorer* esta te indicará el nivel de riesgo de las páginas que se visiten y avisará si detecta que alguna de ellas está destinada al *Phishing*. Su instalación es sencilla y en pocos segundos su puede disfrutar de las posibilidades que nos ofrece. También muestra información adicional acerca de la antigüedad de la página y del servidor que la aloja, de esta forma se podrá reportar páginas que no estén marcadas como maliciosas, y así de esta manera poder avisar a los demás usuarios de esta barra.

- *Phistank*. es una herramienta colaborativa que permite a los usuarios añadir las direcciones pertenecientes a sitios web fraudulentos. Se trata de una base de datos de sitios fraudulentos, aportados por los usuarios, que permitirá ser usadas mediante otros desarrollos gracias a la disposición de una *API* e integrarla en otras herramientas de seguridad. Por lo tanto, esta es una herramienta que permite no sólo verificar si una dirección que viene por correo electrónico pertenece a un sitio fraudulento, sino aportar más información en caso de encontrarnos con un sitio posiblemente fraudulento, verificándolo y siguiéndolo. También dispone de su propio blog y estadísticas.

- *Google Safe Browsing*. Alerta acerca de las páginas que piden datos personales/bancarios haciéndose pasar el banco sin serlo realmente. Con esta extensión atacan al gran problema de los navegadores, la seguridad, siendo el *Phishing* el gran peligro para navegantes. Como siempre, en este tipo de funcionalidades hay que mirar con lupa el tema de la privacidad. Hay que tener en cuenta que para que *Google* analice la veracidad de una web, debe ser informado de la visita. De hecho, con *Google Safe Browsing* guardan si una web ha sido aceptada o rechazada por el usuario tras el aviso de la extensión y, en modo *"Enhanced Protection"* envía cada *URL* que visitamos a *Google*. Eso sí, la empresa del buscador jura y perjura que no asocia estos datos con ninguna *IP*.

- *WOT*. *Web Of Trust* es un complemento para diferentes navegadores que evita caer en sitios peligrosos o de mala reputación. *WOT* puede ser añadido a *Firefox, Internet Explorer o Google Chrome,* cada vez que hagas una búsqueda o visites un sitio web, *WOT* te indicará si el sitio es fiable o no, permite evitar una increíble cantidad de sitios maliciosos: Falsos antivirus, falsos *antispywares*, falsas versiones de programas, sitios fraudulentos, sitios de estafas, páginas con virus, páginas ofreciendo programas conteniendo *troyanos*, páginas que intentan robar contraseñas, páginas para adultos, etc.

- *TrendProtect*: Es un navegador *plugin* gratuito que le ayuda a evitar páginas Web con contenido no deseado y amenazas ocultas. *TrendProtect* revisa la tasa de incidencia actual de la página, de la misma forma revisa las listas de páginas en *Google, MSN*, y los resultados de búsqueda de *Yahoo* para verificar la seguridad de esta misma. Puede utilizar la clasificación para decidir si usted desea visitar o evitar una página Web determinada. *TrendProtect* se basa en una amplia base de datos que cubre el siguiente tipo de información de miles de millones de páginas Web: Categoría de contenido, detección de *Phishing*, reputación del sitio web, etc.

Cabe mencionar algunas aclaraciones importantes para el correcto funcionamiento de este tipo de barras estas son las siguientes:

- No instalar varios complementos ya que podría ralentizar la navegación.

- No instalar cualquier *toolbar* ya que muchas de éstas pueden ser nefastas, es importante primero analizar cuales nos ofrecen protección.
- Muchas de estas barras son propuestas durante la instalación de programas sobre todo gratuitos.
- Si a pesar de tener instalado algún bloqueador de ventanas emergentes te sigue apareciendo publicidad, lo más probable es que tu PC esté infectado. Por lo tanto, analiza tu PC con tu programa de protección o pasa un antivirus en línea.
- Tener instalada una barra no significa que se esté completamente protegido es recomendable que igual se tenga instalado un antivirus para mayor protección.

4.6- Funcionamiento de Web de Confianza (WOT)

A continuación seleccionaremos una barra de herramientas para mostrar el funcionamiento, así como la instalación de esta, seleccionamos la herramienta *WOT* es poderosa y gratuita, con lo cual cualquiera podrá utilizarla de manera eficiente, de la misma forma es de las pocas herramientas que funcionan para: *Firefox, Opera, Internet Explorer o Google Chrome*. Por todo esto la herramienta es muy versátil y la hace un buen ejemplo.

Primero debemos tener en cuenta que la instalación es un poco diferente para cada explorador.

4.6.1 En Firefox.

- Primero haremos click en el menú "Herramientas" y selecciona "Complementos" en la ventana que se abre, haz click en la pestaña "Obtener complementos". Escribe WOT en el recuadro y haz clic en la lupa. Luego haz clic en "Añadir *a Firefox*" como se muestra en la *Figura 4.5*.

Figura 4.5 Búsqueda de WOT en complementos de Firefox.

- Luego haz clic en instalar ahora. Como se muestra en la *Figura 4.6* nos abrirá una ventana de instalación.

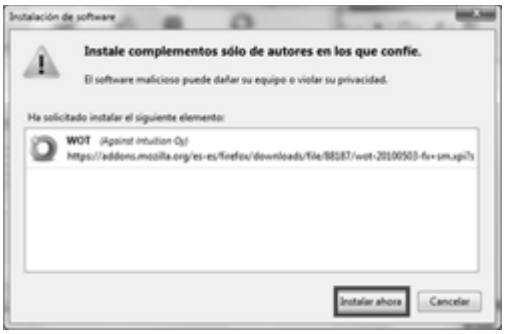


Figura 4.6 Ventana de instalación.

- Haz clic en el botón reiniciar *Firefox*. En la *Figura 4.7* se pude ver claramente como *Firefox* nos pedirá reiniciar antes de terminar la instalación.

Figura 4.7 Ventana solicitando el reinicio de Firefox.

- Acepta la licencia que aparece.
- En la página que aparece puedes seleccionar una configuración o dejar la configuración por defecto y cerrar la ventana haciendo clic en el aspa. En la *Figura 4.8* como se puede apreciar nos solicitara elegir una configuración que creamos adecuada para nuestro programa.

Figura 4.8 Configuración de WOT.

- WOT ya ha sido instalado.

4.6.2 En Internet Explorer.

Para la instalación en Internet Explorer es mucho más simple que en los demás exploradores lo único que debemos de hacer es seguir las siguientes instrucciones:

- Entrar a la siguiente dirección *http://www.mywot.com/en/download/ie*
- Selecciona el idioma y hacer click en el botón "*Free Download for IE*"
- Una vez descargado, se instala y queda todo listo para su uso.

4.6.3 En Google Chrome.

- Haz clic en la llave de tuercas situado en el extremo superior derecho y selecciona "Extensiones". En la *Figura 4.9* podemos ver la forma de empezar la instalación de la herramienta en *Google Chrome*.

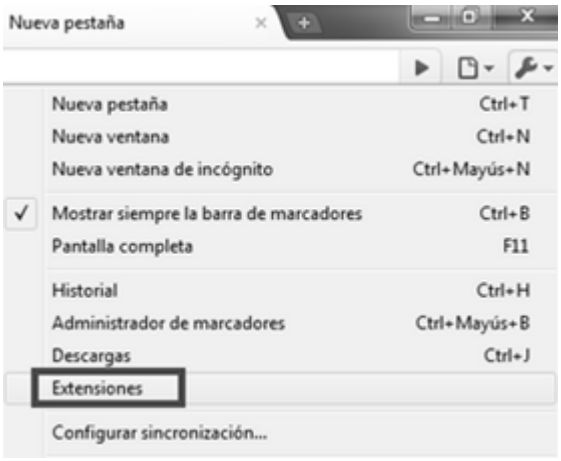


Figura 4.9 Extensiones de Google Chrome.

- En la ventana que se abre, haz clic en "Obtener más extensiones". A continuación en la Figura 4.10 podemos ver como se obtienen más extensiones.

Figura 4.10 Ventana para obtener más extensiones.

- En el cuadro de búsqueda escribe WOT y haz click en la lupa. En la *Figura 4.11* se aprecia que la búsqueda de la extensión y en la *Figura 4.12* se ve como se instala la herramienta.

Figura 4.11 Búsqueda de la extensión WOT.

- En la lista de resultados haz clic en WOT y luego haz clic en "Instalar".

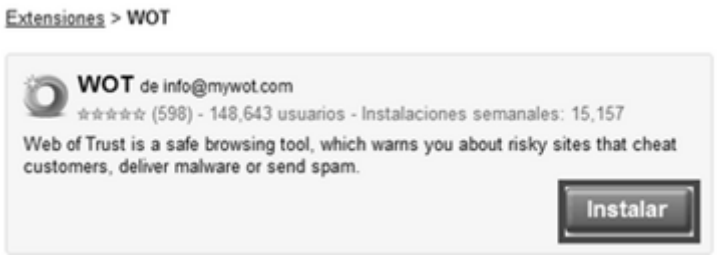


Figura 4.12 Ventana de instalación.

- En la ventana que aparece haz clic en "Instalar" para confirmar la instalación. Ahora en la Figura 4.13 se nota la ultima pantalla para la instalación.

Figura 4.13 Instalación de WOT en Chrome.

- En la página que aparece puedes seleccionar una configuración o dejar la configuración por defecto y cerrar la ventana haciendo clic en el aspa.
- El icono de WOT aparece a la derecha de la barra de direcciones y mediante un código de colores te indica acerca de la fiabilidad de un sitio web.

4.6.4 En Opera.

Copia el archivo javascript. Ponlo en una carpeta de tu elección (por ejemplo, una carpeta dentro de la carpeta Opera)

- Dirígete a "Herramientas > Opciones > Contenidos".
- Haz clic en "Opciones JavaScript".
- En "Carpetas JavaScript de usuario" haz clic en el botón "Seleccionar" y selecciona la carpeta. Luego haz clic en "Aceptar".
- WOT ha sido activado e indicará los sitios dudosos utilizando más de 20 motores de búsqueda.

También puedes entrar a este enlace http://www.mywot.com/en/blog/wot-bookmarklet-for-safari-and-opera debes agregar el enlace "dragging this link to your bookmarks" a los favoritos para que aparezca una ventana emergente que indique la reputación de la página web. En la *Figura 4.14* se puede observar la forma en que se instala WOT en Opera.

Al hacer clic sobre un favorito tendremos:

Figura 4.14 Instalación de WOT en Opera.

Ahora veremos su funcionamiento de WOT con una búsqueda en Google por ejemplo hagamos una búsqueda en Google del término "spybot" esto es lo que obtenemos:

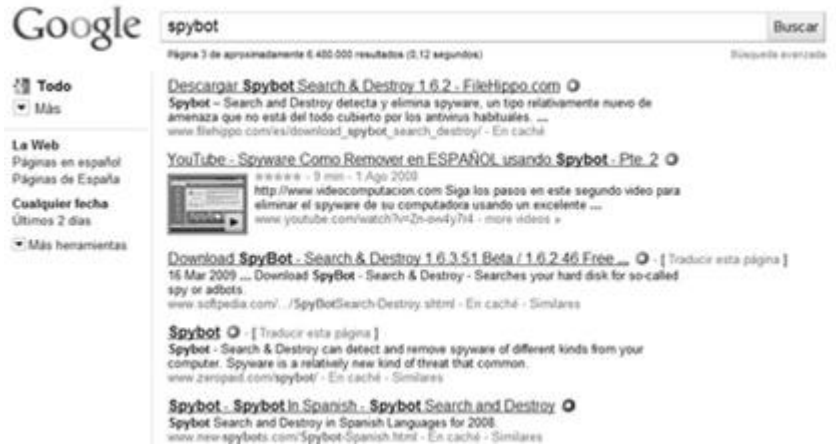


Figura 4.15 Búsqueda en Google con WOT.

A la derecha de cada enlace de la lista de resultados aparece un pequeño círculo de color. Las páginas con círculos rojos deben ser evitadas, las que tienen un círculo verde son fiables como se puede ver en la *Figura 4.15*. A continuación las diferentes evaluaciones que puede mostrar WOT en la *Figura 4.16*.

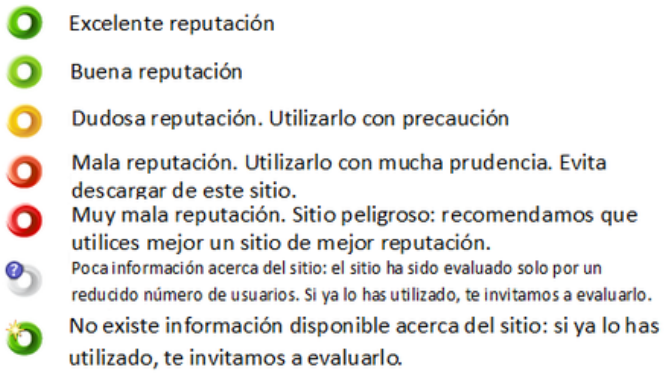


Figura 4.16 Tabla con la forma en que se clasifican los sitios.

Entrando a un sitio Web peligroso simplemente debemos observar el color del círculo situado a la derecha de la barra de direcciones, aparecera un circulo rojo y una advertencia:

Figura 4.17 Advertencia de sitio inseguro.

Es posible registrase en el sitio de WOT, pero no es necesario para beneficiarse de la protección de WOT. Esto te será útil si quieres indicar sitios peligrosos. Podrás evaluar los sitios y añadir comentarios. Evidentemente, en un inicio tu evaluación no tendrá mucho peso. Pero a medida que vayas evaluando los diferentes sitios web tu evaluación tendrá más peso.

CONCLUSIONES

Con base en los objetivos planteados al principio del presente estudio se observa la importancia que tiene la Ingeniería Social y el impacto de esta, en el caso particular del *Phishing*, es de suma importancia tener conocimiento de este tipo de prácticas ya que la información es vital para todos, por este motivo es necesario que la gente tome una serie de precauciones para evitar este tipo de ataques, ya que la desinformación es la principal herramienta que usan los Ingenieros Sociales para sus prácticas.

La Ingeniería Social cambia constantemente adaptándose a los medios que existan, pero si se estudia detenidamente el principio del ataque es el mismo, esta investigación servirá para atacar el fenómeno actual y también predecir el comportamiento que tendrá en el futuro con el nacimiento de nuevas tecnologías.

La definición de Ingeniería Social se confunde con facilidad con el término utilizado por las ciencias políticas el cual nos habla de los esfuerzos y las acciones de los ingenieros por la sociedad, sin embargo, el término informático es totalmente distinto indicándonos que es la práctica de obtener información personal a través de la manipulación.

Phishing es el principal delito de estafa a través de la red en la actualidad, esta se realiza al momento de obtener información de algún usuario y suplantar su identidad en diversos medios como son entidades bancarias en línea, servicios de pagos a través de la red, acceder a diversos tipos de redes sociales, etc.

Es fácil caer en este tipo de prácticas esto debido a que existe una gran desinformación sobre este tipo de delito y la forma de operar de los atacantes algunas de estas son:

1. Correos electrónicos. Usuarios atraídos por una serie de engaños muy simples para ingresar en diversos sitios y obtener su información personal.
2. Suplantación de páginas Web. Se basa en comprar el dominio de una página web que se parezca mucho a la página oficial y de esta forma cuando la gente intente acceder a este servicio la información se le proporcionara al administrador de esta página.
3. Instalación de *malware*. Al acceder a una página o descargar un archivo el equipo se infecta con un programa llamado *keylogger* este graba todo lo que hace el usuario con el teclado y lo envía al correo de la persona que lo programo.
4. *Familiarity Exploit*: Basado en la familiaridad y la confianza que las personas tenemos al reaccionar a peticiones de individuos que nos son relativamente conocidos.

5. T*rashing*: Revisar los desperdicios y la basura nos puede proporcionar información de los usuarios.
6. Robo de información de cuentas bancarias. Se obtiene la información como la clave del usuario y con diversos métodos se obtiene la tarjeta de crédito de la víctima o se clona esta misma después se vacía la cuenta.

A base del estudio también podemos proveer que el siguiente blanco para los hacker son los dispositivos móviles, primeramente porque nadie espera un ataque en su *Smartphone* o en su *Tablet* pero sobre todo que no existen herramientas tan desarrolladas para la seguridad de dispositivos móviles que para computadoras personales, viendo esa deficiencia es importante aplicar buenas prácticas de seguridad en estos dispositivos y no dejar todo el cargo de la responsabilidad a los programas automáticos.

También se observa que mientras más avanzan las tecnologías de comunicación, la gente descuida más su información, esto se debe a que los usuarios dejan toda la responsabilidad de seguridad a herramientas dedicadas a este fin, sin embargo, como se comprobó, un pequeño descuido por parte del usuario es una puerta abierta para el criminal.

Lo anterior da un amplio enfoque, permitiendo entender y correlacionar conceptos que no parecieran tener una relación en primera instancia, los usuarios deben de poner atención sobre a quién proporcionan cierta información personal y en revisar que se hace con esta misma.

Es necesario crear de material como lo es el presente trabajo de tesis, que permita a los estudiantes mantenerse al día con las nuevas tecnologías existentes en materia de seguridad, así como el proveer conocimiento para el uso responsable de la información que esté a su cargo durante su vida profesional.

ANEXOS

Herramientas adicionales para la práctica del Phishing.

Anexo I- Herramientas adicionales para la práctica del Phishing.

Hoy en día se tienen diversas practicas de *Phishing* especializadas en el robo de información en diversos medios electrónicos, sin embargo hay un gran sector que basa esta práctica en la obtención de información de usuarios con tarjeta de crédito, los métodos que se ocupan son muy diversos a continuación mencionaremos algunos de ellos, así como la forma de evitar caer en este tipo de prácticas.

- *Cambiazo*: Este ocurre cuando un cliente realiza una transacción con su tarjeta de crédito en un cajero automático o realiza un pago electrónico con su tarjeta y permite que un tercero le ayuda con la transacción que logra con simples engaños cambiar su tarjeta de crédito y ver su clave personal, para posteriormente realizar operaciones fraudulentas. Algunas recomendaciones para prevenir el cambiazo de tarjeta:

    - No aceptar colaboración de extraños al momento de realizar transacciones con su tarjeta.
    - Desconfíe de la gente que se ofrece a ayudarle.
    - Cuando digite su clave hágalo con precaución y evite que otras personas puedan verla.
    - Cuando retire su tarjeta de un cajero automático, verifique que efectivamente sea la suya y haga lo mismo cuando realice compras en establecimientos.

- *Clonación:* Consiste en la copia de la banda magnética de las tarjetas, puede ocurrir en los cajeros automáticos, establecimientos. Los delincuentes utilizan para esto un dispositivo de tarjetas que copia información solamente deslizando la tarjeta por su ranura, en este método igual deben de instalar un dispositivo extra que será el encargado de copiar la clave. También los delincuentes podrán realizar compras a su nombre falsificando la firma. Algunas recomendaciones para prevenir la clonación.

    - Antes de utilizar un cajero automático verifique que no se encuentre ningún material extraño pegado en la ranura.
    - En caso de encontrar algo sospechoso repórtelo de inmediato a su banco.
    - Si su tarjeta es retenida por el cajero:
        - Repórtelo de inmediato a su banco.
        - No permita ni solicite ayuda apersonas extrañas.

- Cancele la operación que llevaba y repórtelo en el banco.

Para seguir adelante con este anexo primero pasaremos a definir un término importante el cual es *Skimminng*, ya que se trata del método en específico utilizado para la clonación de tarjetas de crédito.

Anexo II- Skimming

Esta práctica es conocida también como clonación de tarjetas de crédito o debito, consiste en la duplicación de tarjetas de crédito o debito sin el consentimiento del dueño de la tarjeta.

El problema con esta práctica es que los dueños de las tarjetas de crédito o debito no se dan cuenta de esto hasta que les llega el estado de cuenta o cuando van a comprar algo en una tienda o por internet con su tarjeta y le dicen que su tarjeta está al límite o se la rechazan.

A continuación mostraremos la forma en que se realiza una clonación de tarjeta de crédito así como un ejemplo real de esta práctica, este manual se encontró en la siguiente página web.
http://foro.elhacker.net/seguridad/skimming_clonacion_de_tarjetas_de_credito-t326739.0.html

1. *En la Figura A.1* el delincuente tiene en su poder un *Skimmer* de bolsillo (usado para leer y guardar la información de la tarjeta).

Figura A.1 Skimmer de bolsillo

2. Posteriormente el delincuente que trabaja en algún establecimiento espera a que alguien vaya a pagar y pasa la tarjeta del cliente por la maquina original del establecimiento y por su *Skimmer* para guardar la información de la tarjeta. En la *Figura A.2* s muestra lo fácil que es usar un *Skimmer*.

Figura A.2 Uso del Skimmer de bolsillo

3. Luego va a su casa y conecta el *Skimmer* a una computadora y pasa la información desde el *Skimmer* hacia la computadora.

4. Luego el delincuente utiliza una tarjeta en blanco con cinta magnética y la pasa por otra máquina llamada codificador de tarjetas de crédito para pasar la información de la computadora hacia la tarjeta en blanco y listo. En la *Figura A.3* se puede ver como usan una tarjeta limpia para poder clonarla.

Figura A.3 Codificador de tarjetas de crédito

Ahora la tarjeta que estaba en blanco posee la información de la tarjeta original, lista para comprar y gastar dinero a su nombre.

De igual manera es prudente mencionar que el *Skimmer*, el decodificador de tarjeta y las tarjetas en blanco pueden ser comprados por internet por cualquier persona.

Estos son los pasos que toman los delincuentes para clonar las tarjetas físicamente, si el delincuente solo quiere comprar por internet y no clonar la tarjeta físicamente, llegaría hasta el paso numero 3.

Para evitar ser víctima del *Skimming* se recomienda:

- Cuando termine de comer en un restaurante vaya usted mismo y pague la cuenta antes de irse. El mesero no lo puede obligar a usted a que le entregue la tarjeta para cobrarle.
- Cuando pague en una tienda, preste mucha atención de por donde el empleado pasa la tarjeta, no pierda de vista su tarjeta. Es recomendable estar atento sobre las manos del empleado algunos *Skimmers* son sumamente pequeños y pueden caber en la palma de la mano.
- Cuando vaya a introducir su número secreto (*PIN*) en un cajero cubra con su otra mano el cuadro de botones, ya que los delincuentes instalan pequeñas cámaras que apuntan hacia el cuadro de botones para ver el número secreto que usted entra.
- Cuando vaya a retirar dinero de los cajeros asegúrese de que no tenga ningún dispositivo extraño instalado por donde se introduce la tarjeta. Si sospecha de algo extraño notifíqueselo inmediatamente al gerente del banco o el encargado del establecimiento.
- Si su banco ofrece servicios online aproveche esta ventaja ya que le permite a usted monitorear sus estados de cuentas y transacciones diariamente, así no tendría que esperar hasta que le llegue su estado de cuenta para verificar si hay alguna compra, retiro de dinero o transacción sospechosa.
- Antes de introducir su tarjeta, verifique que ningún elemento obstruya la ranura, modifique su clave de acceso periódicamente.
- Si la luz ubicada sobre la ranura para el ingreso de la tarjeta es de color rojo, no utilice el cajero automático, no olvide terminar la sesión antes de abandonar el cajero automático.

Como se menciono con anterioridad es importante resaltar este tema debido a que obtener lo necesario para la clonación es cosas sumamente sencilla, a continuación mostraremos un kit que se vende por internet para poder clonar tarjetas.
Para esto se visito el sitio *http://bogotacity.olx.com.co/vendo-kits-para-clonar-tarjetas-de-credito-iid-66668554*
La información que nos proporciona el vendedor es la siguiente: Nuevo modelo *Skimmer* KORO-16 está diseñado para trabajar con prácticamente todos los modelos de cajeros automáticos. Esto es posible gracias al extremadamente pequeño tamaño de *skimmer* koro-16, así como a las nuevas tecnologías (nuevas soluciones para la transmisión Bluetooth se han utilizado en el producto, así como la más nueva tecnología para la lectura de la pista electromagnética por medio de los rayos infrarrojos junto con la cabeza lectora de *Blu-ray Imán* (*BDM*) estándar. En la *Figura A.4* se ve lo compacto y portátil de un *Skimmer portátil* el cual tiene la misma dimensión que el groso de la cinta magnética de las tarjetas de crédito.

Figura A.4 Skimmer portátil

El *software* permite a los equipos de doble dirección-tira magnética lectura; lectura que sucede que no demora, ni detiene la interrupción de la tarjeta de crédito, por lo que la lectura es de 100%. Hemos hecho alrededor de 10.000 intentos - todos los resultados fueron exitosos. Gracias al tamaño extremadamente pequeño de skimmer puede trabajar con modelos de cualquier cajero automático, así como con cualquier otro dispositivo que soporte de banda magnética.

El proceso de instalación es muy sencillo; un lado de la KORO-16 está equipado con una almohadilla auto despegable, lo que permite conectarlo en el cajero. Es igualmente fácil desmontar el dispositivo para recargar la batería. (Cargador incluido). El tiempo mínimo de carga KORO-16 es de 24 horas.

Figura A.5 KORO-16

El siguiente elemento del dispositivo - «baseEXP-16»:
«BaseEXP-16» - recibe la señal Bluetooth de skimmer KORO-16 y, a continuación, procesa la señal y envía SMS con PISTA 1 TRACK2 y PIN (de pinpad)-información que llega a su teléfono celular (cualquier número de cualquier compañía de telefonía celular). El *SMS* contiene el texto cifrado (caótico letras y números) que se puede descifrar con la ayuda de nuestro software (la aplicación "CODE-16" es fácil de instalar en Windows XP y Vista) en el hogar en el equipo. Tiempo de carga de la batería es de 30 horas (cargador incluido). La *Figura A.6* muestra el esquema del funcionamiento del kit.

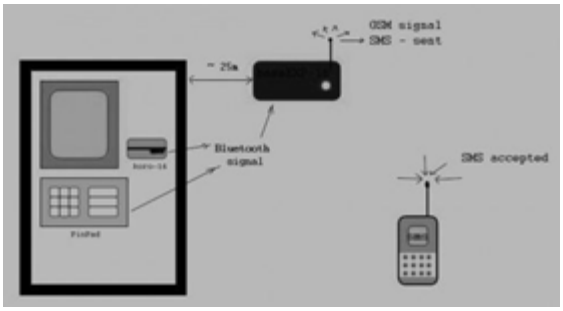


Figura A.6 Esquema de funcionamiento del kit.

El siguiente componente *PinPad*.
Importante: *PinPad* - es fabricado individualmente para cualquier modelo de cajero automático.

Instalación:

1. Inserte tarjeta *SIM* (de cualquier número de cualquier compañía de telefonía celular) en «baseEXP-16».

2. Conecte «baseEXP-16» a su PC vía cable USB, ejecute "CODE-16" y el tipo de solicitud en el número de teléfono que desea recibir información.
3. Después de instalar *skimmer* KORO-16 y la «baseEXP-16» en cualquier lugar dentro del radio de 25 metros (garantizado radio Bluetooth para recibir la señal es de 25 metros de la *skimmer* KORO-16). Esto no te dará ningún tipo de dificultades, ya que el «baseEXP-16» es bastante pequeño. En la *Figura A.7* muestra un teclado falso apra poner encima del cajero y poder registrar las claves.

Figura A.7 PinPad

Para terminar nos informa del costo del producto y el envió.

- El precio de este kit de productos es de $800 usd.
- Sin costo de envío.
- Cada producto viene con sus manuales respectivos.
- Garantía de 12 meses.
- Asesoría telefónica por 3 meses.

El envío demora 48 después de haber hecho el depósito o giro bancario se envía por la empresa de mensajería *DHL* a cualquiera parte de Colombia y América las ventas no son de entrega inmediata ya que es muy importante mantener la confidencialidad de nuestra ubicación exacta.

Anexo III- Clonación de tarjeta de crédito por medio de la compañía de mensajería.

Ahora revisaremos un nuevo método de clonación que ha surgido en la actualidad, esta técnica es preocupante debido a que la duplicación de tarjetas de crédito es más fácil de realizar, para ello los delincuentes copian las tarjetas antes de que lleguen al usuario, haciendo inútil la prevención por parte de los clientes. La *Figura A.8* hace referencia a las tarjetas de crédito que son clonadas antes de llegar a sus dueños legítimos.

Figura A.8 Tarjeta de crédito clonada

Para ello se solicita una tarjeta de crédito, inadvertidamente el dueño de la tarjeta la recibe al poco tiempo y se olvida de ella, al poco tiempo le llega el estado de cuenta y observa que tiene registrados varios gastos a pesar de nunca haber usado la tarjeta. Investigaciones que realizaron los bancos revelaron que la banda magnética de la tarjeta ya no es clonada durante una transacción, sino que es clonada antes de que el dueño la reciba.

Las tarjetas llegan a terceros antes que a los dueños por lo tanto los delincuentes las mantenían en su poder, las clonan y posteriormente la envían a los dueños y ellos no tienen idea de que su tarjeta ha sido clonada por delincuentes que están dentro de la compañía de mensajería, de esta forma los métodos de prevención son ineficaces y dejan sumamente vulnerable a las personas para ser víctimas de clonación.

Tablas

GLOSARIO

Definiciones y conceptos utilizados en el presente trabajo.

A

ADWARE: Programa que tiene como finalidad mostrar o bajar publicidad. Estos programas normalmente se instalan cuando se instala o se ejecuta otra aplicación.

ANDROID: Sistema operativo basado Linux diseñado para dispositivos móviles, tales como smartphones, posteriormente se expandió su desarrollo para soportar otros dispositivos tales como tablet pc , reproductores MP3, netbook, PC, televisores, etc.

ANTIVIRUS: Aplicación cuya finalidad es la detección y eliminación de virus, troyanos y gusanos informáticos.

ANTIVIRUS BASADO EN LA NUBE: Software que tiene las mismas funciones que un antivirus convencional pero que en vez de almacenar definiciones de virus en la computadora, el antivirus manda información a través de Internet a los servidores de las compañías para su análisis.

API: Interfaz de programación de aplicaciones (del inglés Application Programming Interface) es el conjunto de funciones y procedimientos o métodos, en la programación orientada a objetos que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción.

B

BANCA ELECTRÓNICA: Hace referencia a los servicios bancarios que se ofrecen a través de Internet, estos pueden tener una sucursal física o solo operar de esta manera.

BLUETOOTH: Especificación para redes inalámbricas de área personal que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia en la banda de los 2,4 GHz. Los dispositivos que con mayor frecuencia utilizan esta tecnología pertenecen a dispositivos móviles como PDA, teléfonos, computadoras portátiles y Tablet PC.

C

CIBERTERRORISMO: Uso de un medio electrónico con el fin de causar terror en una población con fines políticos, económicos o religiosos.

CORREO ADJUNTO: Archivos anexos enviados junto a un correo electrónico, suelen ser una forma común de propagación de virus de computadora.

COMANDOS AT: Grupo de comandos desarrollados para la comunicación con los modems, que fueron adaptados para ser usados en la telefonía. Todos los teléfonos móviles disponen de un juego de comandos AT especificos que permiten su configuración y realizar llamadas de voz o datos, escribir y enviar mensajes SMS, leer y escribir en la agenda de contactos.

CRACKEO: Parche diseñado para que un programa tenga distinto compartimiento, como validar software fraudulento o activar software gratis.

CRACKER: Personas que se dedican a explotar las vulnerabilidades de un sistema con fines maliciosos.

D

DATOS PERSONALES: Es cualquier información relacionada con el usuario, por ejemplo, el nombre, teléfono, domicilio, fotografía o huellas dactilares, así como cualquier otro dato que pueda servir para identificar. Este tipo de datos te permiten además, interactuar con otras personas, o con una o más organizaciones.

DELITO INFORMÁTICO: Delito cometido utilizando una computadora; también se entiende por delito informático cualquier ataque contra un sistema computarizado.

DIRECCIÓN IP (INTERNET PROTOCOL): Conjunto de cuatro números del 0 al 255 únicos e irrepetibles con el cual se identifica una computadora conectada a una red que corre el protocolo IP.

DISPOSITIVO MÓVIL: Son aparatos de pequeño tamaño, con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, con memoria limitada, diseñados específicamente para una función, pero que pueden llevar a cabo otras funciones más generales, por ejemplo teléfonos inteligentes, Tablet PC o palms.

DNS (DOMAIN NAME SERVICE): Sistema que asocia información variada con nombres de dominios asignados a cada uno de los participantes. Traduce nombres comunes de dominios a direcciones IP y localiza servidores de correo electrónico.

E

ESTÁNDAR: Norma que se utiliza como punto de partida para el desarrollo de servicios, aplicaciones y protocolos.

ERROR DE SOFTWARE (BUG): Resultado de un fallo o deficiencia durante el proceso de desarrollo de creación software.

EXPLOIT: Método de utilizar un bug o fallo para penetrar en un sistema.

F

FAMILIARITY EXPLOIT: Técnica de ingeniería social que se basa en establecer un circulo cercano y ganar la confianza de la persona que se intente atacar.

FEED WEB: Es un medio de redifusión de contenido web, se utiliza para suministrar información actualizada frecuentemente a sus suscriptores.

FIREWALL: Software y hardware de seguridad encargado de chequear y bloquear el tráfico de la red. Sistema que se coloca entre una red e Internet para asegurar que todas las comunicaciones se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, anti-virus, autenticación, etc.…

G

GUSANO: Malware que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

H

HACKER: Persona que accede a un sistema informático sin autorización para ver su funcionamiento interno y explotar vulnerabilidades.

HOST: Equipos que ofrecen servicios de transferencia de archivos, conexión remota, servidores de base de datos, servidores web, etc. Los usuarios que hacen uso de los hosts pueden a su vez pedir los mismos servicios a otras máquinas conectadas a la red. De forma general un host es todo equipo que posee una dirección IP y que se encuentra interconectado con uno o más equipos.

HTML (HYPERTEXT MARKUP LANGUAGE): Lenguaje de programación que se utiliza para el desarrollo de páginas de Internet. Se trata de la sigla de HyperText Markup Language, es decir, Lenguaje de Marcas de Hipertexto. EL HTML permite describir la estructura y el contenido en forma de texto, además de complementar el texto con objetos tales como imágenes.

I

INGENIERÍA SOCIAL: Es el conjunto de técnicas destinadas a explotar las vulnerabilidades de seguridad de un sistema a través de usuarios legítimos.

ISP (INTERNET SERVICE PROVIDER): Empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como DSL, Cable módem, GSM, Dial-up, Wifi, entre otros.

J

JAVA SCRIPT: Es un lenguaje de programación interpretado orientado a objetos basado. Utiliza principalmente en su forma del lado del cliente (client-side), implementado como parte de un navegador web permitiendo mejoras en la interfaz de usuario y páginas web dinámicas, aunque existe una forma de Java Script del lado del servidor (Server-side Java Script o SSJS). Su uso en aplicaciones externas a la web, por ejemplo en documentos PDF, aplicaciones de escritorio (mayoritariamente widgets) es también significativo.

K

KEYLOGGER: Software o un dispositivo específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un archivo o enviarlas a través de internet. Permite que otros usuarios tengan acceso a contraseñas importantes, como los números de una tarjeta de crédito, u otro tipo de información privada que se quiera obtener.

M

MALWARE: Es un término genérico utilizado para describir el software malicioso tales como: virus, troyanos, etc.

MENSAJERÍA INSTANTÁNEA: Forma de comunicación en tiempo real entre dos o más personas basada en texto. El texto es enviado a través de dispositivos conectados a una red como Internet.

METASPOILT: Es un proyecto de código abierto de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad y ayuda en pruebas de penetración y en el desarrollo de firmas para Sistemas de Detección de Intrusos.

N

NAVEGADOR WEB: Aplicación que opera a través de Internet, interpretando la información de archivos y sitios web para que podamos ser capaces de leerla. El navegador interpreta el código, HTML generalmente, en el que está escrita la página web y lo presenta en pantalla permitiendo al usuario interactuar con su contenido y navegar hacia otros lugares de la red mediante enlaces o hipervínculos.

NUBE: Servicio que funciona a través de internet que permite a los usuarios guardar información cualquier tipo: música, videos, en General y poderlos tener alojados en servidores dedicados, es decir en equipos que siempre permanecen encendido.

P

PAYPAL: Empresa estadounidense, propiedad de eBay, perteneciente al sector del comercio electrónico por Internet que permite la transferencia de dinero entre usuarios que tengan correo electrónico. PayPal también procesa peticiones de pago en comercio electrónico y otros servicios webs, por los que cobra un porcentaje.

PENT-TEST (PENETRATION TEST): Procedimiento metodológico y sistemático en el que se simula un ataque real a una red o sistema, con el fin de descubrir y reparar sus problemas de seguridad.

PHARMING: Variante de Phishing que consiste en suplantar el sistema de resolución de nombres de dominio (DNS) para conducir al usuario a una página web falsa.

PHISHING: Técnica de la Ingeniería Social que consiste en la suplantación de sitios de Internet, se puede presentar en correos electrónicos y páginas web fraudulentas que aparentan proceder de instituciones de confianza como bancos o instituciones públicas.

PHP: Lenguaje de programación interpretado, diseñado originalmente para la creación de páginas web dinámicas. Se usa principalmente para la interpretación del lado del servidor pero actualmente puede ser utilizado desde una interfaz de línea de comandos o en la creación de otros tipos de programas incluyendo aplicaciones con interfaz gráfica.

PROTOCOLO: Estándar establecido. En lo referente a conectividad de redes, el empleo de un protocolo se realiza para direccionar y asegurar la entrega de paquetes a través de la red.

PYTHON: Es un lenguaje de programación de alto nivel cuya filosofía hace hincapié en una sintaxis muy limpia. Este es un lenguaje de programación multiparadigma ya que soporta orientación a objetos, programación imperativa y, en menor medida, programación funcional.

R

RED SOCIAL: Sistemas o estructuras sociales en los que se realiza un intercambio entre sus miembros, y de los miembros de una red con los de otra, que puede ser otro grupo u otra organización. Esta comunicación dinámica permite sacar un mejor provecho de los recursos que poseen los miembros de estas redes. Los individuos o miembros son llamados "actores" o "nodos" en las publicaciones que detallan el funcionamiento de las redes sociales, y se llama "aristas" a las relaciones entre ellos. Las relaciones entre los miembros de las redes sociales pueden girar en torno a un sin número de situaciones tales como el intercambio de información, el financiero, o simplemente la amistad o las relaciones amorosas.

REDES ZOMBIES: Es la denominación que se asigna a computadoras personales que tras haber sido infectados por algún tipo de malware, pueden ser usadas por una tercera persona para ejecutar actividades hostiles. Este uso se produce sin la autorización o el conocimiento del usuario del equipo. El nombre procede de los zombis o muertos vivientes esclavizados, figuras legendarias surgidas de los cultos vudú.

ROOTKITS: Conjunto de herramientas usadas por los intrusos informáticos o crackers que consiguen acceder ilícitamente a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos.

S

SEGURIDAD INFORMÁTICA: Área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta implementando una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

SET (SOCIAL ENGINEERING TOOLKIT): Conjunto de herramientas diseñadas por David Kennedy para realizar ataques automatizados por medio de ingeniería social métodos como la clonación de sitios web para realizar ataques o ataques mediante el envió de un archivo de formato por medio de correos electrónicos.

SKIMMING: Esta práctica es conocida también como clonación de tarjetas de crédito o debito, consiste en la duplicación de tarjetas de crédito o debito sin el consentimiento del dueño de la tarjeta.

SKYPE: Software que permite comunicaciones de texto, voz y vídeo sobre Internet. Esta aplicación también incluye una característica denominada YY SkypeOut,2 que permite a los usuarios llamar a teléfonos convencionales, cobrándoseles diversas y bajas tarifas según el país de destino, pudiendo llamar a casi cualquier teléfono del mundo. Otra opción que brinda Skype es SkypeIn, gracias a la cual se otorga un número de teléfono para que desde un aparato telefónico se pueda contactar cualquier equipo. Además, se provee de un servicio de buzón de voz.

SMARTPHONE: Teléfono móvil que ofrece más funciones que un teléfono celular común. Casi todos los smartphones soportan completamente un cliente de correo electrónico con la funcionalidad completa de un organizador personal además permiten la instalación de programas para incrementar el procesamiento de datos y la conectividad. Estas aplicaciones pueden ser desarrolladas por el fabricante del dispositivo, por el operador o por un tercero.

SMS (SHORT MESSAGE SERVICE): Servicio disponible en los teléfonos móviles que permite el envío de mensajes de texto entre teléfonos móviles, teléfonos fijos y otros dispositivos móviles.

SNIFFER: Programa que captura datos dentro de una red de cómputo; es utilizado por los hackers para obtener nombres de usuarios y contraseñas además permite auditar e identificar paquetes de datos en un red, misma que, puede ser usado legítimamente por los administradores de redes y personal de mantenimiento para identificar problemas de la misma red.

SPAM: Mensajes no solicitados, no deseados o de remitente no conocido, habitualmente de tipo publicitario, generalmente enviados en grandes cantidades que perjudican de alguna o varias maneras al receptor.

SPEAR PHISHING: Variante del Phishing tradicional destinada a conseguir datos de toda una organización o de un grupo de personas.

SPIM: Correo basura que se propaga a través del servicio de mensajería instantánea.

SPIT (SPAM OVER INTERNET TELEPHONY): Son mensajes pregrabados que se distribuyen automáticamente por medio de VoIP.

SPYWARE: Pequeñas aplicaciones cuyo fin es el de obtener información, sin que el usuario se dé cuenta, de tipo comercial. Generalmente se encuentran dentro de aplicaciones gratuitas en Internet.

T

TÉCNICA DE SALAMI: Se utilizan para desviar pequeñas cantidades de bienes de una fuente con un gran cantidad de los mismos; de la misma forma que de un salami se cortan pequeñas rodajas sin que el total sufra una reducción considerable, un programa salami roba pequeñas cantidades de dinero, de forma que su acción pasa inadvertida.

TRASHING: Se refiere a buscar información en la basura de las empresas con el objetivo de encontrar información valiosa acerca de la empresa o, en el mejor de los casos, encontrar claves y contraseñas.

TROYANO: Programa informático cuya ejecución tiene unos efectos imprevistos y, generalmente, insospechados para el usuario infectado. No se les puede denominar virus porque no se replican.

U

URL (UNIFORM RESOURCE LOCATOR): Secuencia de caracteres, de acuerdo a un formato modélico y estándar, que se usa para nombrar recursos en Internet para su localización o identificación, como por ejemplo documentos textuales, imágenes, vídeos, presentaciones, presentaciones digitales, etc.

V

VENTANA EMERGENTE: Ventanas que emergen automáticamente (generalmente sin que el usuario lo solicite). A menudo, las ventanas emergentes se utilizan con el objeto de mostrar un aviso publicitario de manera intrusiva.

VIRUS: Programa que está diseñado para copiarse a sí mismo sin conocimiento del usuario y con la intención de infectar el sistema operativo y/o aplicaciones, cuyos efectos pueden variar dependiendo de cada virus: mostrar un mensaje, sobrescribir archivos, borrar archivos, enviar información confidencial mediante emails a terceros, etc.

VOIP (VOICE OVER INTERNET PROTOCOL): Tecnologías que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP. Se envía la señal de voz en forma digital, en paquetes de datos, en lugar de enviarla en forma analógica a través de circuitos utilizables sólo por telefonía convencional.

W

WI-FI (WIRELESS FIDELITY). Es el nombre “comercial” con el que se conoce a todos los dispositivos que funcionan sobre la base del estándar 802.11 de transmisión inalámbrica.

BIBLIOGRAFÍA Y MESOGRAFÍA

Recursos impresos y digitales utilizados para el presente trabajo.

Hadnagy Christopher (2011) Social Engineering The Art of Human Hacking, EEUU, Wiley Publishing inc.

Mitnick D. Kevin (2002) The art of deception, EEUU, Hyperion.

IFAI (2004) Transparency, access to information and personal data, México D.F., IFAI

Instituto de acceso a la información pública del Distrito Federal (2008) Ley de protección de datos personales para el Distrito Federal, México D.F.

https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/iberoamerica/proyectos/common/pdfs/Iniciativa-de-Ley-Federal-de-Proteccin-de-Datos-Personales--ap-original-cp-.pdf

http://seguridad.cudi.edu.mx/congresos/2003/cudi2/legislacion.pdf

http://es.wikipedia.org/wiki/C%C3%B3mputo_forense

http://es.wikipedia.org/wiki/Sniffer

http://www.enterate.unam.mx/Articulos/2003/octubre/delitos.htm

http://www.diputados.gob.mx/LeyesBiblio/pdf/113.pdf

http://www.hackhispano.com/foro/showthread.php?t=35795

Descripción de trojano para el fishing
http://www.securelist.com/en/descriptions/161696/Trojan-Spy.HTML.Fraud.gen.

spam en el 2011
http://www.viruslist.com/sp/analysis?pubid=207271129

kaspersky presenta informe de spam del primer trimestre del 2011
http://www.kaspersky.com/sp/news?id=207732905

Encabeza México propagación de troyanos bancarios en AL
http://www.bsecure.com.mx/ultimosarticulos/encabeza-mexico-propagacion-de-troyanos-bancarios-en-al/

Spam reglamentación en México
http://www.ramonbecerra.com/spam-reglamentacion-en-mexico/

Engaño de phishing en facebook
http://www.netmedia.info/featured/nuevo-engano-de-phishing-avisa-que-cancelaran-perfiles-de-facebook/

Microsoft confirma ataques de phishing a Xbox life
http://www.bsecure.com.mx/ultimosarticulos/microsoft-confirma-ataques-de-phishing-a-usuarios-de-xbox-live/

Sony disculpa por hackers
http://www.bsecure.com.mx/ultimosarticulos/ceo-de-sony-se-disculpa-y-hackers-planean-un-tercer-ataque-contra-psn/
http://www.bsecure.com.mx/ultimosarticulos/nuevo-ciberataque-a-sony-estima-perdidas-anuales-por-3200-mdd/

Victimas de ciberfraudes no lo denuncian por vergüenza
http://www.bsecure.com.mx/ultimosarticulos/victimas-de-ciberfraudes-no-denuncian-por-verguenza/

Subdirección de Seguridad de la Información
Información y servicios de seguridad en computo (UNAM)
http://www.seguridad.unam.mx/index.html

http://www.cert.org.mx/index.html

http://www.pcworld.com/article/182180/top_5_social_engineering_exploit_techniques.html

Condusef
http://www.condusef.gob.mx/

SET: Kit de herramientas para Ingeniería Social
http://foro.cibernodo.net/tema-set-kit-de-herramientas-para-ingenier%C3%ADa-social

SET: Kit de herramientas para Ingeniería social
http://www.daw-labs.com/set-kit-de-herramientas-para-ingenieria-social/

Canal de Phishing
http://www.canal-ayuda.org/a-virus/phishing.htm

Phishing en Paypal
http://www.muyinternet.com/2011/07/04/phishing-paypal

Keylogger
http://es.wikipedia.org/wiki/Keylogger

Facebook y Mesenger nuevas vías para el phishing
http://www.rfsdigital.com/2010/03/facebook-y-messenger-nuevas-vias-para.html

URL obfucation
http://www.contentverification.com/obfuscation-attacks/

http://seguridadblanca.blogspot.com/2010/01/analisis-phishing-de-msn.html

Herramienta de google contra el phishing
http://www.spamspam.info/2009/07/17/google-integra-una-herramienta-contra-el-phishing-relacionado-con-ebay-y-paypal-en-gmail/

Barras de protección para tu navegador
http://es.kioskea.net/faq/4853-barras-de-proteccion-para-tu-navegador-web

URLVOID
http://www.urlvoid.com/

Phishing fraude electrónico
http://gdata-antivirus.blogspot.com/2008/04/phishing-o-fraude-electrnico.html

Como se hace phishing
http://ingenieriasocialsigloxxi.wordpress.com/category/3-como-se-hace-ing-social/3-1-phishing/

Clonación
http://www.grupobancolombia.com/seguridades/laClonacion.asp

Cambiazo
http://www.grupobancolombia.com/seguridades/cambiazo.asp

Phishing en Facebook
http://spamloco.net/2011/10/phishing-de-facebook-con-mensajes.html

Ataque de phishing en Twitter
http://geeksroom.com/2011/07/severo-ataque-de-phishing-en-twitter/51507/

Ataque de phishing dirigido contra la Dirección General de Trafico
http://www.muycomputerpro.com/2011/01/19/nuevo-ataque-de-phishing-dirigido-contra-la-direccion-general-de-trafico/

Paypal phishing
http://luctus.es/2011/10/paypal-phishing/

Aplicación falsa de Netflix
http://antivirus.es/falsa-aplicacion-de-netflix-roba-datos-de-usuarios-4081

Soldados americanos victimas de phishing
http://antivirus.es/los-soldados-norteamericanos-son-las-nuevas-victimas-del-%e2%80%9cphishing%e2%80%9d-3211

StalTrak nuevo fraude en Twitter
http://antivirus.es/cuidado-con-staltrak-nuevo-fraude-en-twitter-3671

Vishing
http://antivirus.es/vishing-phishing-a-traves-de-tecnologia-voip-3384

Phishing utilizando McDonalds
http://www.techweek.es/seguridad/noticias/1009263004801/cibercriminales-utilizan-mcdonalds.1.html

Vulnerabilidad en American Express
http://www.tendenciadigital.com.ar/seguridad/noticias/descubierta-vulnerabilidad-en-sitio-de-american-express-que-permite-phishing.html

Dr. Web para Firefox
http://es.kioskea.net/faq/4855-dr-web-para-firefox-para-mayor-seguridad

Netcratf Toolbar
http://netcraft-toolbar.uptodown.com/

WOT
http://es.kioskea.net/faq/4874-wot-complemento-para-evitar-caer-en-paginas-peligrosas
http://www.trendsecure.com/portal/en-US/tools/security_tools/trendprotect

Antivirus basado en la Nube
http://www.tecnocosas.es/cloudav-ultima-tecnologia-antivirus-online/
http://www.infospyware.com/blog/argumentos-en-contra-de-los-antivirus-en-la-nube/
http://www.eecs.umich.edu/fjgroup/cloudav/

Antivirus móviles
https://seguridadpcs.wordpress.com/2011/09/11/la-importancia-de-la-seguridad-en-los-dispositivos-moviles-smartphones-y-tablets/
http://exgoe.com/hackers-los-dispositivos-moviles-y-las-redes-sociales.html