Federación Latinoamericana de Bancos

XX CELAES 2005

Comité de Expertos en Seguridad Bancaria

Guatemala, Guatemala

Agosto 10 - 12, 2005

PHISHING

IMPACTO NEGATIVO EN EL SISTEMA BANCARIO

Robo de Identidad, nuevo reto de seguridad

1. **Marco de Referencia y Definición de Conceptos**
2. **Análisis y Tratamiento de la Evidencia Digital**
3. **"Phishing Scam"**
4. **Herramientas Forenses**
5. **Recomendaciones del uso de Internet en la Banca**

- DELITO CIBERNÉTICO
- DELITO ELECTRÓNICO
- DELITO INFORMÁTICO

COMPUTO FORENSE

- IDENTIFICACIÓN
- PRESERVACIÓN
- EXTRACCIÓN Y ANÁLISIS
- PRESENTACIÓN

Lic. Carlos Ramírez Acosta, CPP, CPO.
PRISMA Consulting Services
prismacarlos@avantel.net
Agosto 11 de 2005
15:00 a 16:30

1. Marco de Referencia y Definición de Conceptos

Qué es *phishing*

La aparición de esta palabra norteamericana recientemente en el ámbito de la seguridad de la información en el mundo de habla hispana define la duplicación de un original de una página web, normalmente de bancos con fines delictivos.

El "phishing" consiste en el envío masivo de mensajes electrónicos con falsos remitentes que aconsejan a los usuarios que rellenen y confirmen los datos y contraseñas para poder acceder a sus cuentas bancarias.

El término "phishing" puede ser la contracción de "password harvesting fishing" (cosecha y pesca de contraseñas) y, a pesar de que este término data de mediados de los años 90 en Estados Unidos, es ahora cuando empieza a oírse en castellano.

No existe de momento una definición al español pero hay algunos términos que podrían servir como posibles sustitutos: delito informático, correo electrónico fraudulento, ciberestafa o fraude por Internet.

La Fundación del Español Urgente aconseja que se mantenga este término en inglés escrito en cursiva o entre comillas y se aclare su significado (entre paréntesis), siempre que sea posible, con alguno de los términos ya citados.

Como consecuencia de los altos niveles de fraude mediante "phishing" en los Estados Unidos de Norteamérica, se considera esta modalidad criminal como "robo de identidad automatizada".

Este delito informático combina el poder de la red Internet con la candidez y/o codicia de la naturaleza humana para defraudar a millones de personas y por lo tanto millones de dólares.

Tan sólo en ese país se estimaban pérdidas el año 2004 de unos $2.4 billones de dólares (www4.gartner.com/Init), en donde casi dos millones de personas dieron sus datos personales bajo la modalidad de “phishing”.

Casi cualquier persona en el mundo con una dirección electrónica habrá recibido a la fecha algún tipo de “email” con propósitos fraudulentos. Estos mensajes de correo utilizan el formato y apariencia típica de una institución legítima que la hacen parecer confiable para que los usuarios proporcionen su claves de acceso y contraseñas de sus cuentas bancarias.

El problema en estos casos es que no se esta comunicando con una organización legitima real. La información obtenida engañosamente podrá ser utilizada para acceder a las cuentas bancarias del usuario, realizar transacciones sin autorización y además crear nuevas cuentas.

Algunos términos

Cracker.- Un hacker delincuente o “black hat”. Alguien con las habilidades y conocimientos para llevar a cabo serios ataques a los sistemas computaconales.

Hacker.- Alguien con mucho talento y dominio con los sistemas computacionales que le agrada penetrarlos pero no necesariamente con fines criminales.

Mula.- Alguien cuya cuenta bancaria es utilizada para lavar dinero por medio del “phishing”.

Phish.- Una victima que proporciona información a un “phisher”.

Phisher.- Un ciber delincuente cuyo “modus operandi” es el “phishing”.

Phishing.- El acto de engaño de obtener información personal directamente por el uso de Internet.

Phishing email.- Un mensaje de correo electrónico enviado a víctimas potenciales.

Phishing scam.- Un conjunto de acciones fraudulentas, usualmente un mensaje de correo electrónico y una página web.

Phishing spyware.- Programas espía utilizados para robar información personal dentro de un esquema de "phishing scam". Esta modalidad va desde los dispositivos "keyloggers" hasta programas sofisticados que "miran" aquellos sitios web que han sido visitados por los usuarios.

Phishing website.- Un sitio o página web que recolecta información personal a través de "phishing".

Nota Especial

Por considerarlo de gran importancia se recomienda que el lector de este documento tenga ocasión de revisar el reporte original adjunto del "Anti-Phishing Workin Group" (APWG), que muestra un detalle del problema y el resultado de los estudios y tendencias analizadas al mes de Junio de 2005.

En otro orden de ideas…

El desarrollo de este trabajo no se centra en concepciones de naturaleza legal propias del campo jurídico, sino sólo como un referente para enfatizar la importancia de las acciones irregulares, ilícitas y dolosas donde intervienen los dispositivos computacionales y/o de comunicaciones, bien sea como objetivo de la acción ("en contra de"), o como medios comisivos de conductas antisociales ("por medio de"), que ponen en riesgo y, en su caso, afectan los intereses patrimoniales y otros valores de la sociedad.

En tal sentido, pretendemos dar una idea clara de los principales conceptos vinculados con el tema de los delitos cibernéticos y la computación forense, especialmente, en esta ocasión, con el llamado “Phishing”. (Ver anexos al final de este trabajo y consultar página www.antiphishing.org)

Definiciones básicas

Delito.- Acción u omisión voluntaria o imprudente penada por la ley.

Cibernética.- Estudio de las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas; y en particular, el de las aplicaciones de los mecanismos de regulación biológica a la tecnología.

Electrónica.- Estudio y aplicación del comportamiento de los electrones en diversos medios, como el vacío, los gases y los semiconductores, sometidos a la acción de campos eléctricos y magnéticos.

Informática.- Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras.

Computación.- Someter datos al tratamiento de una computadora.

Forense.- Perteneciente o relativo al foro. Usualmente, presentaciones ante autoridades legales en un foro para discernir y resolver sobre un asunto técnico.

Adoptando recientes estudios jurídicos realizados en México y Argentina en materia de delitos “en contra de” y “por medio de” computadoras, haremos un breve repaso.

El marco conceptual “en contra de” y “por medio de”

Muy difícil resulta alcanzar una exacta delimitación de la significación de los conceptos. Para tales efectos, se distinguen las siguientes construcciones gramaticales.

a. Delitos cometidos por medio de elementos electrónicos
b. Delitos cometidos en contra de equipos electrónicos
c. Delitos cometidos por medio de elementos informáticos
d. Delitos cometidos en contra de equipos informáticos

Mediante procedimiento de descarte, se tiene que:

1. Se advierte que todos los equipos informáticos están construidos con elementos electrónicos, y que no todos los equipos electrónicos son necesariamente equipos informáticos (Ejemplo: radio o televisor), por lo que corresponde dejar de lado la opción “d”, toda vez que la misma se encuentra contenida dentro de la “b” la cual, a su vez, es más amplia en su encuadre de interpretación.
2. También se observa que sólo los equipos dotados de la capacidad de procesar datos pueden, por regla general, ser utilizados como medio comisivo de acciones que afecten bienes jurídicos que a la sociedad le pueda interesar brindarle mayor protección (la penal), ya que resulta muy difícil imaginar a un sujeto activo tratando de, por ejemplo, violar la cerradura electrónica de un banco por medio de una radio o un teléfono celular (que son claros ejemplos de equipos electrónicos no informáticos), pero es fácil imaginar al mismo sujeto activo intentando similar acción por medio de un equipo portátil de procesamiento de datos u otro artefacto similar con la capacidad necesaria para generar en cortos lapsos infinidad de claves numéricas.

Así se descarta la fórmula “a” por resultar poco apropiada a los medios habituales de comisión de delitos, y asimismo por estar alejada de la realidad.

Quedan vigentes las formulaciones “b” y “c”, es decir, delitos cometidos en contra de equipos electrónicos y delitos cometidos por medio de elementos informáticos. Esto marca una notable diferencia entre las alocuciones utilizadas como delitos electrónicos y delitos informáticos.

Se tiene entonces que, los delitos cometidos en contra de equipos electrónicos son aquellos en los cuales el receptor físico del daño perpetrado resulta expresamente un equipo electrónico.

Muy cuestionable sería dentro de esta categoría pretender, incluir el delito específico de daños, reconocido en todas las legislaciones penales, por ejemplo, en aquellos casos en que alguien destruye un cajero automático, salvo que éste tuviere que ver con destrucciones totales o parciales producidas a través de la utilización de medios informáticos.

En contraposición se observan los delitos cometidos por medio de elementos informáticos, los cuales presentan una variada gama que pasa por los daños, las injurias y calumnias, las estafas (por ejemplo, subastas fraudulentas on-line), entre muchos otros.

¿Cuál es el bien jurídico tutelado en cada caso? En el primero se advierte que es la integridad física y lógica de los equipos electrónicos, y por ende el derecho de propiedad del sujeto pasivo. En el segundo, se advierte que son múltiples las posibilidades de bienes jurídicos a proteger y altamente distintos entre sí, como el honor la protección de datos, el patrimonio, etc.

Determinando el bien jurídico protegido, puede inducirse que, en el caso de los delitos informáticos, los múltiples posibles, ya se encuentran en su mayoría protegidos por medio de figuras como el robo, la estafa, las injurias y calumnias, etc., contenidos en códigos penales o leyes especiales.

En resumen, al perpetrarse el delito a través del uso de medios informáticos no se está sino en presencia de un nuevo método comisivo del delito y no, como erróneamente se piensa, ante un nuevo delito, ya que para que lo sea debe estar correctamente tipificado.

Los delitos informáticos, en su gran mayoría, dependen, para su persecución penal, de la correcta interpretación de la ley penal y de la toma de conciencia por parte de los jueces de que sólo nos encontramos ante nuevos métodos para estafar o para injuriar, pero en ningún caso ante nuevos delitos, ya que una postura semejante llevaría al absurdo de pensar, por ejemplo, que si mañana pudiese quitar la vida a alguien por medio de la Internet habría que establecer una nueva figura penal, ya que el homicidio no estaría cubriendo esta posibilidad; cuando en derecho, si se lesiona el bien jurídico protegido, no importa cuál sea el medio utilizado, corresponde la aplicación de la ley penal vigente y no se requiere una nueva y específica.

En este punto, queda por analizar el caso de aquellos delitos que no se encuentran tipificados, ya que no corresponden a bienes jurídicos protegidos, al menos a primera vista, como el caso específico del “hacking” u otros similares.

Nos encontramos dentro del ámbito específico de los que son delitos electrónicos, por el tipo de bien afectado que pueden ser el delito de daños, para el que por regla general no existe legislación.

Para estos casos particulares se requiere una rápida acción del legislador para definir los tipos penales y agregarlos a los vigentes, sin perjuicio de que al hacer las respectivas modificaciones, y según la legislación de cada país, puedan agravarse algunos tipos existentes en función del uso de nuevas tecnologías para, de esta forma, desalentar su utilización indebida.

Puede establecerse que:

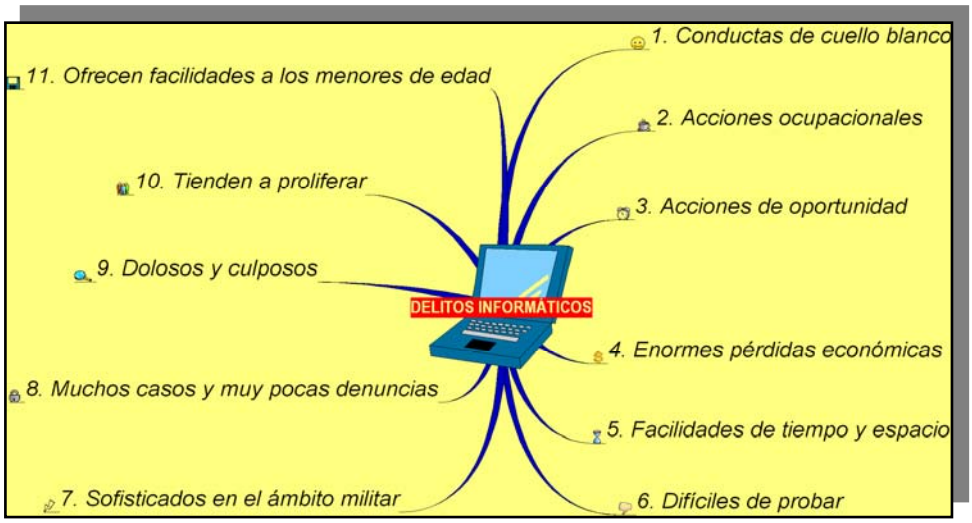
1. Los delitos electrónicos e informáticos no resultan equivalentes y además los términos no son sinónimos.
2. Todos los delitos electrónicos son perpetrados por medio del uso de la informática, razón por la cual no cabe menos que inferir que los delitos electrónicos son una especie del género de los informáticos.
3. En la mayoría de los casos, los delitos electrónicos constituyen una especie tan particular y específica que a la fecha, no encuentran dentro del espectro penal vigente la protección del bien jurídico que se afecta, mientras que los delitos informáticos la poseen, ya que no son otra cosa que nuevos medios comisivos de delitos ya existentes.
4. Siguiendo esta línea de reflexión puede precisarse que el género delito informático reconoce, al menos dos especies.
    - Delitos informáticos electrónicos
    - Delitos informáticos no electrónicos.

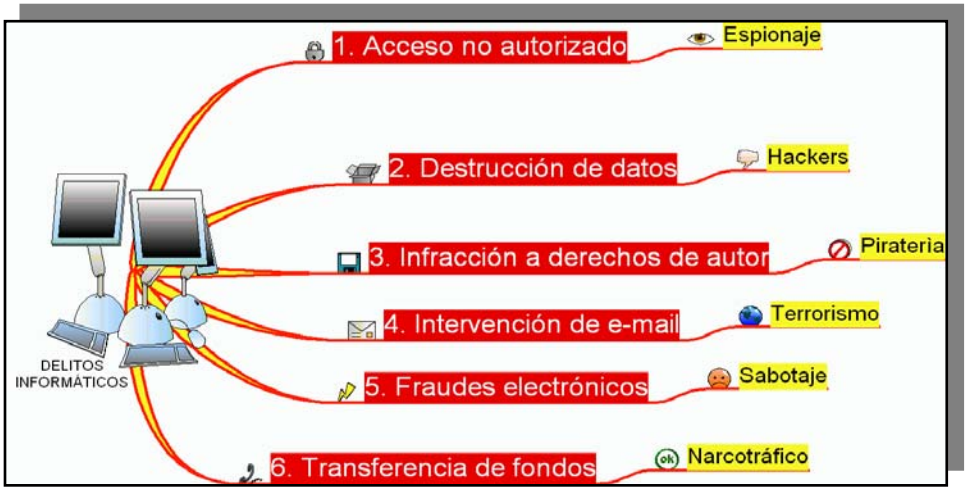
Algunas definiciones convencionales recomendadas:

- **Delitos Informáticos**: Son todos aquellos en los cuales el sujeto activo lesiona un bien jurídico, que puede o no estar protegido por la legislación vigente y que puede ser de diverso tipo, por medio de la utilización indebida de medios informáticos.
- **Delitos Electrónicos o Informáticos Electrónicos:** Son una especie del género de los delitos informáticos en los cuales el autor produce un daño o intromisión no autorizada en equipo electrónicos ajenos, y que a la fecha, por regla general, no se encuentran legislados, pero que poseen como bien

jurídico tutelado, en forma específica, la integridad de los equipos electrónicos y la intimidad de sus propietarios.

- **Delitos Cibernéticos:** Son ilícitos en que se tiene a las computadoras como instrumento, medio o como fin.





2. Análisis y Tratamiento de la Evidencia Digital

El presente apartado pretende dar a conocer de una manera sencilla, los principales conceptos y recomendaciones en torno al manejo de las evidencias electrónicas generadas por la comisión de conductas ilícitas en el campo de las ciencias computacionales.

Esto es, las prácticas consideradas como las mejores para la cadena de custodia de la evidencia digital, que puede encontrarse en el lugar de los hechos de un delito cibernético. Se trata de material de orientación que sintetiza varias concepciones investigadas y aplicadas por el autor.

- El término “delito cibernético” no se encuentra tipificado como tal en nuestros códigos punitivos, pero no es una limitante para comprender la dimensión del concepto y las consecuencias respecto de los actos irregulares o ilícitos informáticos que se cometen con las computadoras.

- Como un ejemplo, vale la pena precisar que en el Código Penal Federal Mexicano, se encuentran 7 artículos que tratan el tema del **acceso ilícito a sistemas y equipos de informática**, que en alguna medida son análogos al concepto típico de un delito cibernético. (Título Noveno del CPF, Arts. 211 Bis 1 al 211 bis 7)

En América Latina, los ataques e incidentes criminales relacionados con sistemas de cómputo se han incrementado y nadie es inmune a la amplia gama de actos maliciosos de los pillos informáticos, por tanto, la seguridad en cómputo debe apreciarse como un problema de personas y de procesos que puede solucionarse con la conciencia del problema y con la tecnología, resultando a veces necesaria la aplicación de técnicas de investigación criminal y de análisis forense.

El mundo en línea y los diferentes tipos de crímenes que se cometen en la supercarretera de la información representan una nueva frontera dentro de las comunicaciones electrónicas, de tal manera que los retos y desafíos para analistas e investigadores, hoy día, están vinculados con el aseguramiento y preservación de evidencia relacionada con las computadoras, así cómo saber reaccionar y responder ante un crimen cibernético.

- En este sentido, es menester comprender que identificar y seguir la pista a la evidencia digital y protegerla, es la parte crucial de un programa de mejores prácticas en materia de cómputo forense.

- La evidencia digital puede estar contenida en la computadora de la víctima o en un dispositivo de almacenamiento como un disquete; en los archivos del proveedor de servicios de internet (ISP); en la computadora del victimario o sus disquetes, o bien en otras ubicaciones del ciberespacio. Pero donde quiera que se encuentre la evidencia habrá que tratarla con extremo cuidado.

- Una evidencia es todo aquel elemento generado en la comisión de una conducta delictiva que proporciona información para soportar conclusiones, hallazgos y recomendaciones relacionadas con un hecho que se investiga.

La evidencia digital es frágil, sensible y volátil. Puede destruirse o alterarse con facilidad. Puede encontrarse en múltiples ubicaciones. Pero una regla básica que cualquier persona debe conocer es que si una computadora involucrada en un incidente criminal esta apagada ésta no debe encenderse, y si esta encendida no debe apagarse sin las indicaciones de algún especialista.
En un caso extremo, si es imprescindible apagar una computadora es preferible desconectarla de la fuente de corriente de la parte trasera de la máquina y no del suministro eléctrico, pues puede estar conectada a un dispositivo de respaldo de energía y en ese momento la evidencia podría afectarse haciéndola invalida para un proceso legal. De estos tópicos tratará este artículo.

El ciber crimen

Si bien la investigación criminal es un proceso cuya metodología aplicada en la práctica resulta esencial para la resolución exitosa de cualquier tipo de ilícito, ahora, con el surgimiento e innovación vertiginosa de las tecnologías de los sistemas de información y de telecomunicaciones, se hace necesario que los analistas e investigadores tengamos al alcance herramientas apropiadas y procedimientos concretos para atender y esclarecer la diversidad de conductas ilícitas que se generan, como resultado del uso de ambientes informáticos o, simplemente del uso de computadoras personales con fines criminales.

- Una estrategia de investigación efectiva es la aplicación de una metodología de tratamiento de ilícitos que comprende las siguientes cuatros fases: **exploratoria, confirmatoria, comprobatoria y resolutiva.**

- En la primera, se identifica y dimensiona el problema a resolver, en la segunda se confirman o descalifican las hipótesis planteadas, en la tercera se prepara el paquete de pruebas y en la cuarta se toman decisiones legales, administrativas, técnicas, de control y de seguridad.

- En nuestro país, una de las actividades especializadas que esta empezando a ser demandada tanto por organismos policiales como por empresas de cualquier giro y tamaño que utilicen computadoras o redes computacionales, es la práctica de la **computación forense**, disciplina técnica que desde el punto de vista de la investigación criminal y del campo pericial podemos situarla dentro del espectro de la criminalística y las ciencias forenses.

- Para analistas e investigadores avanzados que realizan diligencias de computación forense, existen en el mercado varios programas de software para el tratamiento de la evidencia digital, tal es el caso de “EnCase”, “Safeback” y “FTK”, herramientas desarrolladas para recuperar datos borrados, archivos ocultos, crear imágenes forenses, esto es “clonar” el disco duro para un análisis detallado de su contenido digital.

Conviene aclarar que las conductas delictivas, antisociales o contraproductivas que en los últimos años vienen investigando las autoridades policiales que cuentan con unidades de policía cibernética, como por ejemplo, la pornografía infantil por internet, las amenazas y riesgos asociados del correo electrónico, la piratería informática, la clonación de teléfonos celulares, el robo de señales de las compañías televisoras, entre otros incidentes, sólo forman parte del amplio abanico de riesgos y amenazas potenciales que suceden en la red y con las computadoras, sin que estén realmente definidos como delitos cibernéticos, ya que por el tipo de bien jurídico que tutelan corresponden a otro delitos debidamente tipificados en nuestras leyes.

- Ante este escenario, es posible identificar ciertas acciones dolosas donde los equipos informáticos son usados específicamente como medio, método o fin de un delito, o transgresión de una norma interna de una organización y, que tal conducta pueda requerir de una determinada sanción penal o administrativa, si

logra configurarse la tipicidad del hecho, bien sea por la acción u omisión de una conducta registrada.

- Podemos decir, que en materia de las mejores prácticas para el tratamiento de cualquier tipo de evidencia y, ahora dentro del campo de la computación forense, **la regla más importante sigue siendo la protección de la evidencia, ya sea física o digital.**

¿Cómo se define al cómputo forense?

Una de las definiciones que podemos considerar como universal señala que se trata del proceso de aplicación de técnicas científicas y analíticas a infraestructura de cómputo, para identificar, preservar, analizar y presentar evidencia de manera que sea aceptable en un procedimiento legal.

- El término "forense" proviene de foro -sitio donde los tribunales juzgan las causas- implica un ejercicio y aplicación de índole técnica y de procedimientos mediante los cuales se aprovechan una o varias ramas de la investigación criminal o de ciencias conexas que estudian y resuelven casos concretos ligados habitualmente a situaciones legales o jurídicas.
- Lo forense es también establecer premisas y fundar conclusiones específicas, amoldándolas para ello a un proceso, siguiendo un método estructurado de tal manera que permita formular una resolución expresada en términos técnicos.

Coincido con la opinión de algunos profesionales de la seguridad informática en cuanto a que el cómputo forense, no obstante su carácter terminal jurídico, puede también utilizarse como un efectivo proceso de aclaración interno de incidentes computacionales de riesgo antisocial, errores o negligencia, al interior de las organizaciones, realizando un reporte discrecional hacia las autoridades públicas, dado que puede haber razones de peso estratégico que afectarían la continuidad operativa, viabilidad e imagen de una organización en particular si se revelase información sensible sobre sistemas o aplicaciones vulneradas.

Lo que en efecto es imperativo hacer, es documentar, aclarar, resolver y reparar la situación del riesgo informático materializado e instaurar los controles detectivos internos y mecanismos de monitoreo para un tratamiento preventivo y de respuesta inmediata ante un eventual ataque posterior.

Tomemos nota que los delitos informáticos son cometidos por personas y no por las máquinas y que de acuerdo a diferentes estudios publicados se estima que en materia del ciber crimen el enemigo realmente puede estar en casa. En lugar de analizar sólo las herramientas tecnológicas para descubrir las fallas, es necesario comprender que las estadísticas recientes indican que de cada 10 incidentes criminales relacionados con computadoras, 7 de ellos son cometidos con la complicidad de algún empleado de la compañía afectada.

Por lo tanto, es sumamente importante la investigación de todo el recurso humano vinculado directa e indirectamente en un incidente criminal detectado.

La criminología y los ciber criminales

Las conductas delictivas son una creación de la naturaleza humana. El modo en que nos comportamos los seres humanos cotidianamente depende de una serie de factores genéticos, físicos, psíquicos y ambientales que aun son un misterio. En este sentido y pese a que existen estudios serios sobre el perfil del ciber criminal, la naturaleza humana es cambiante, evolutiva y exploradora, por lo que también debemos estar atentos con los modelos tradicionales de evaluación criminológica del delincuente y ajustar o generar nuevos modelos, de ser el caso, para tratar a los ciber criminales.

Al intentar analizar a un delincuente informático, debemos también hablar del concepto personalidad, terreno complementario al campo técnico del análisis forense de las computadoras. Sin embargo, no podemos sustraernos del tema puesto que la investigación de un delito cibernético nos refiere un acto humano y la computación forense, un análisis de las máquinas, esto es, al estudio conjugado del hombre y de la máquina.

Si la definición común de personalidad establece que se trata de la organización más o menos estable y duradera del carácter, temperamento, intelecto y físico de una persona que determina su adaptación única al medio ambiente, entonces podemos extrapolar y sustentar como hipótesis que para tratar de entender la personalidad del delincuente informático, asumiendo que antes de serlo se conducía dentro de lo que entendemos por normalidad, debemos advertir rasgos de desviación y ciertos cambios en el carácter,

temperamento, procesos de aplicación cognitivos y modificación en la apariencia física. Cambios que en nuestro medio conocemos como “Red Flags”.

Ahora bien, tomemos en cuenta la extraordinaria habilidad que demuestra una inteligencia superior compleja, de aquellos individuos de tal pericia en el uso de sistemas y programas computacionales, llamados hackers, phreakers y crackers, que conforman capacidades individuales y en ocasiones comunidades expertas, cuyos intereses en la computación pueden ser la aplicación de su inteligencia para demostrar su superioridad dado el reto irresistible que les causa vulnerar y penetrar las redes informáticas.

Aquí, es donde debemos estar conscientes de nuestras limitaciones de análisis y de investigación para completar y compensar nuestra fuerza sumando los talentos de otras personas con sus especialidades para contrarrestar posibles embates de transgresores informáticos superiores.

- El típico perfil del hacker señala que se trata de individuos inquietos, curiosos, creativos, lectores ávidos, conocedores avanzados técnicamente, clasemedieros económicamente y anarquistas. Es un perfil que aparecerá con más frecuencia dadas las facilidades y ola tecnológica por la que atravesamos en el mundo entero. Es decir, estemos alertas y sigamos profesionalizando la labor del analista e investigador en tareas de delitos cibernéticos y cómputo forense.

- También, cada vez es más popular escuchar el término de **ingeniería social**, refiriéndose a la actividad de engaño que desarrollan algunas personas especialmente del mundo de los sistemas, para hacerse de claves confidenciales, información privilegiada, o simplemente de datos sensibles para fines ilícitos.

Esto habla igualmente de un nivel intelectual orientado a la manipulación de alto nivel, utilizando mecanismos de seducción y engaño y probablemente a la existencia de carisma y personalidad mágica. Pero también revela al estudioso de la mente una suerte de rasgos psicopatológicos que pueden capitalizarse por los profesionales de la seguridad informática.

Por tanto, es de utilidad no sólo el conocimiento especializado en sistemas computacionales, sino también el de las ciencias como la criminología y la criminalística, al trabajo colegiado de especialistas de diferentes ramas del saber de la prevención y la seguridad, pública o privada.

En síntesis, la investigación de un delito cibernético y la computación forense se desarrollan trabajando en equipo.

Procedimientos para el aseguramiento de equipo de cómputo y tratamiento de la evidencia digital

"Las evidencias son testigos mudos que no mienten". Esta máxima establece un principio fundamental, y en materia de cómputo forense ya se trate de evidencias físicas, como huellas, herramientas, hardware, cables, documentos, manuales, etc., o evidencias digitales, como programas de software, registros de acceso (logs), archivos informáticos, imágenes de computadora, etc., siempre habrá que hacer los mejores esfuerzos para proteger la evidencia.

- La diferencia entre una evidencia física y una digital es que ésta última es frágil, sensible y volátil y puede contaminarse o destruirse permanentemente afectando completamente el resultado de un caso.

- La mejor manera de asegurar que la evidencia física o digital de un delito cibernético ha sido debidamente (1) identificada, (2) preservada, (3) analizada para (4) presentarla como prueba legal, se conoce como "cadena de custodia".

- La **cadena de custodia** implica un extremo cuidado desde el momento en que se llega a la escena del crimen o lugar de los hechos, se fijan fotográficamente, levantan y embalan los indicios o evidencias identificadas obrando registro de día, hora, condiciones especiales, pero sobre todo, de las personas que participan y tienen cualquier tipo de contacto o control de la evidencia hasta que se deposita en el laboratorio o lugar apropiado para su análisis y custodia, así como de las veces que se utilice como prueba durante diligencias judiciales (o

análisis y demostraciones administrativas internas en ambientes controlados y monitoreados de empresas afectadas).

Introducción

Primeramente hay que señalar que es conveniente establecer contacto y suscribir acuerdos de cooperación con una Unidad de Policía Cibernética, por ejemplo en México, existe un comité especial denominado **Grupo Delitos Cibernéticos México** (integrado por representantes de los sectores público y privado que analizan y promueven acciones de combate a estos ilícitos), o de un Equipo de Respuesta a Incidentes de Cómputo (como el CERT-UNAM), con quienes se tenga un enlace y comunicación directa para atender un ilícito informático. Si no existe alguna relación con estas fuerzas de tarea, entonces es conveniente saber de alguna firma consultora o persona especializada que pueda orientar sobre los pasos básicos para proteger la escena del crimen computacional y las evidencias identificadas en el lugar de los hechos o en el lugar del hallazgo.

- Llamamos “lugar de los hechos”, al sitio en donde sabemos se cometió un ilícito y, “lugar del hallazgo”, al sitio en donde se descubrió o detectó el ilícito.
- La Unidad de Policía Cibernética (UPC), el Equipo de Respuesta a Incidentes de Cómputo (ERIC), o algún especialista en prevención e investigación criminal o en seguridad informática (ESP), constituyen apoyos para las áreas de investigación involucradas en delitos cibernéticos.

Debido a la sofisticación de los sistemas y equipos, así como a la habilidad que puede tener un sospechoso de alterar o borrar evidencias rápidamente, es altamente recomendable que el primer hombre en llegar a la escena de un supuesto crimen informático, retire a personas, asegure el lugar, busque y solicite la presencia y asistencia de un miembro de la UPC, o del ERIC, o de un especialista en sistemas.

Esta acción es más fácil y exitosa, si esta considerada en la fase de planeación previa a la intervención y cumplimiento de una orden judicial.

Planeación de una Investigación

Es necesario anticiparse a la realización de un crimen computacional y planear qué va a hacerse en caso de que éste se presente, ya que generalmente son los propios empleados los que están involucrados.

Cuando se presenta un crimen computacional, inmediatamente debe asumirse el control físico, técnico y administrativo del lugar, a través de un grupo de respuesta, que en el caso de una empresa debería incluir participantes de seguridad en sistemas, auditoria interna, recursos humanos, investigaciones corporativas y soporte técnico.

Sobre la premisa probada de un aseguramiento cuidadoso de una computadora o red de computadoras, un laboratorio de cómputo forense aceptará la evidencia y desarrollará un análisis basado en la información que le provea el analista o investigador a cargo de un caso.

Tipología de Delitos con Computadoras

Los crímenes computacionales se definen dentro de tres categorías:

1. La computadora puede ser el objetivo de un crimen como robarla, destruirla o utilizarla sin acceso autorizado. *(Equipo informático usado como fin)*
2. La computadora puede ser la herramienta del crimen como el caso del uso de Internet para enviar pornografía infantil, fraudes informáticos o amenazas y hostigamiento. *(Equipo informático usado como medio)*
3. La computadora puede ser utilizada para almacenar evidencia de un delito como transacciones por lavado de dinero, narcotráfico o registros sensibles apropiados ilícitamente. *(Equipo informático usado como método)*

Tipología de Configuraciones de Computadoras

Los tipos de sistemas de configuración de computadoras que pueden encontrarse en la escena del crimen o lugar de los hechos, pueden variar desde asistentes personales conocidos como PDA´s (Personal Digital Assistants), hasta redes corporativas.

Las categorías más comunes a encontrar pueden ser las siguientes:

1. Computadoras portátiles, laptops o asistentes personales tipo palm pilot o pocket PC.
2. Computadoras personales o que operan como estaciones de trabajo “stand alone”, donde el resto del equipo, programas de software y documentación se encuentran físicamente en un sólo lugar. Este es un escenario típico comúnmente para llevar a cabo un aseguramiento judicial en un departamento, una casa o negocio pequeño. Sin embargo, otros medios de almacenamiento, por ejemplo de contrabando, pueden ser ocultos en cualquier otro lugar.
3. Un sistema de computadora en una casa o negocio pequeño que tiene algunos dispositivos localizados en áreas adyacentes de un inmueble. Como ejemplo, puede darse el caso de un sospechoso que tiene una cámara de video digital en una habitación que se encuentra conectada a un sistema de cómputo en otro cuarto, de tal manera que realice grabaciones pornográficas y las imágenes sean transferidas fácilmente a otras computadoras a través de Internet.
4. Un sistema de red de computadoras en donde múltiples usuarios comparten recursos informáticos y componentes tales como un servidor, o servidores que son computadores optimizados para proveer servicios a otros equipos conectados entre sí. Ese escenario es más parecido al que puede encontrarse en una empresa comercial donde el aseguramiento judicial de todo el hardware puede causar la paralización de operaciones de la compañía y la evidencia culpable puede estar solamente contenida en una máquina. En estas circunstancias, un especialista en seguridad informática podría ser convocado para que desarrolle un análisis en el sitio sobre el equipo que debe ser asegurado bajo el supuesto de una orden judicial.
5. Un sospechoso puede utilizar medidas extremas para ocultar evidencia. De allí el porqué de las precauciones a través de un cuidadoso y completo aseguramiento son muy importantes. Esto refleja también la necesidad de que

una adecuada orden judicial de amplio espectro pueda cubrir los imponderables y no limitarse en la búsqueda física en un sólo lugar. Un especialista en seguridad informática y cómputo forense podrá desarrollar un análisis efectivo y determinar aquella evidencia significativa.

Supuestos

1. El aseguramiento de tipo legal para incautar evidencia relacionada con equipo de cómputo aplica a computadoras personales que no están en red.
2. Si varios sistemas deben ser asegurados, cada sistema deberá ser analizado independientemente.
3. Los analistas o investigadores deben notificar a algún supervisor cuando los procedimientos conocidos aquí referidos no se ajusten a situaciones excepcionales para tomar providencias mayores.
4. Deberán estar contemplados los recursos necesarios anticipadamente para realizar un aseguramiento efectivo.
5. Es recomendable que se designe personal para las siguientes tareas:
    a. Determinar en dónde se encuentra la evidencia
    b. Registrar y documentar el cuarto bajo inspección
    c. Registrar y documentar el área donde se encuentra el cuarto bajo inspección.
    d. Documentar y asegurar la evidencia
    e. Resguardar la evidencia
    f. Registrar e inventariar la evidencia (fecha, hora, lugar, responsable)

Panorama Funcional

Un aspecto importante es que el aseguramiento de una computadora puede no reflejar específicamente la ubicación de la evidencia. Sin embargo, la evidencia potencial de la escena del crimen deberá asegurarse para ser turnada a una entidad especializada, como por ejemplo, un laboratorio de informática forense para su debido tratamiento.

Al ingresar a la escena del crimen, el analista o investigador puede suponer que una computadora personal es independiente, pero en realidad esta conectada a una red. Puede que también el propietario haya preparado al sistema para dañarse si algunas condiciones se suceden fuera de su control.

Por lo tanto, es importante primeramente determinar:

1. SI el ambiente de la escena del crimen es seguro para el analista o investigador
2. Que la computadora no esta dañando la información.
3. La existencia de otras conexiones de equipo hacia otras áreas.

Las tareas primarias para el aseguramiento pueden resumirse de la siguiente manera:

a) Determinar en dónde puede encontrarse la evidencia. Cierto equipo puede estar localizado en zonas adyacentes. Identificar las conexiones para localizar la evidencia.
b) Registrar y documentar la habitación donde la evidencia fue detectada. Esto incluye elaborar diagramas o dibujos que faciliten una mejor comprensión, así como tomar fotografías del lugar. Observar si existen conexiones a través de paredes o pisos.
c) Registrar y documentar el área en donde la evidencia fue encontrada. Esto incluye fotografías y diagramas de cualquier tipo de evidencia física, conexiones y puertos de comunicación.
d) Documentar y asegurar la evidencia. Esto incluye fotografías, dibujos, diagramas y colocar etiquetas de identificación a los equipos y dispositivos detectados.

Documentar y asegurar la evidencia:

A. Equipo.- Computadoras y dispositivos periféricos. Esto incluye la unidad central de proceso y los dispositivos externos como modems y medios de almacenamiento. Es difícil obtener evidencia de dispositivos periféricos como impresoras o escáneres que no almacenan información después de que éstos son apagados. No obstante, puede no ser necesario asegurar estos dispositivos a menos que se requiera analizar otro tipo de evidencias como huellas digitales, por ejemplo. Tome note que cuando se aseguren dispositivos como asistentes digitales personales (PDA´s), alguna información puede perderse si la vida de las baterías se ha agotado. Es importante, por lo tanto, colocar siempre unas baterías nuevas.

B. Líneas telefónicas, cables de conexión.- Deben etiquetarse ambos extremos de líneas telefónicas o cables y marcarse junto con la correspondiente entrada de corriente a la máquina y pared.
C. Los conectores del equipo deben ser igualmente etiquetados aun y cuando éstos no sean utilizados.
D. Conviene colocar una etiqueta que indique “vacio” para identificar un conector o puerto que no este en uso.
E. Medios de almacenamiento.- Asegure todos los disquetes encontrados, cd´s, dvd´s, y cualquier otro dispositivo, aun y si aparentemente parecen dañados o nunca usados. Cuidadosamente registre su posición o ubicación y etiquete estas evidencias.
F. Software.- El software comercial deberá ser también asegurado incluyendo la documentación relacionada.
G. Manuales.- Todos los manuales del lugar de los hechos deben asegurarse.
H. Notas.- Los registros de notas deben también asegurarse ya que pueden contener claves de acceso (passwords) u otra información relevante.
I. Comunicaciones.- Se incluyen modems externos o faxes o grabadoras telefónicas. De ser posible, recupere cualquier número telefónico marcado.
J. Otros.- Verifique el área en general en busca de evidencia potencial.
K. Toda la evidencia identificada deberá ser cuidadosamente empacada para su transportación.
L. El equipo de cómputo y medios de almacenamiento deberá envolverse en material antiestático preferentemente.

Herramientas del analista – investigador

a. Estuche de desarmadores
b. Lámpara
c. Cinta de aislar
d. Carpeta de dibujo
e. Cámara con diferentes capacidades de tomas para acercamientos y vistas generales
f. Suficientes disquetes formateados y cd´s, dvd´s
g. Marcadores de tinta permanente y de agua
h. Cables
i. Etiquetas de diferentes tamaños
j. Tijeras
k. Guantes
l. Cajas de diferentes tamaños
m. Envolturas antiestáticas
n. Bolsas de papel
o. Baterías suficientes
p. Cinta para marcar evidencia

Protección del lugar de los hechos

- Mantenga al sospechoso o sospechosos alejado de la computadora bajo investigación. Este alerta respecto a que la tecnología inalámbrica disponible actualmente permite activaciones remotas.
- Si detecta la existencia de alguna indicación de destrucción de un programa de software en curso, desconecte de inmediato el cable de conexión detrás de la máquina y documente la información que pueda observar en la pantalla de la computadora.
- Si el monitor muestra algún tipo de información desplegada tome una fotografía.
- Si no es identificable la información registrada en la fotografía, entonces copie manualmente la información observable.

- Si la computadora esta encendida (luz de indicación o ventilador operando), observe si algo parece estar ejecutándose en la computadora, por ejemplo, música o un módem funcionando.
- Desconecte el cable de corriente de la parte de atrás de la computadora.

Búsqueda

- Analice el lugar de los hechos para detectar cualquier posible ataque potencial a los analistas o investigadores presentes.
- Analice el equipo y todas las conexiones para determinar qué es lo que realmente debe ser asegurado.
- Tenga precaución si detecta algún equipo o dispositivo útil para análisis de huellas digitales u otro tipo de indicios.
- Tome fotografías del área y del lugar especifico de los hechos.
- Realice un dibujo y/o diagrama del lugar de los hechos.
- Tome fotografías de la computadora y sus alrededores.
- Realice un diagrama del área de la computadora en cuestión.
- Tome fotografías de todas aquellas áreas donde se encuentren manuales, disquetes y programas de software.

Aseguramiento

- Fotografíe todos los lados de la computadora y del equipo periférico conectado.
- Haga un diagrama de las conexiones de todos los equipos incluyendo los cables, puertos vacíos y posición de los switches y líneas de comunicación conectadas.
- Etiquete todos los puertos usados o no de todo el equipo de cómputo identificado en el lugar de los hechos.
- Vuelva a fotografiar las conexiones, pero ahora con las etiquetas colocadas en los dispositivos.

- Desconecte sólo aquello que es necesario para la transportación, pero etiquete todos los cables, líneas de comunicación en ambos lados de la conexión.
- Si es posible, determine y observe si existe una línea de comunicación funcionando.
- Retire cualquier medio de almacenamiento como disquetes, cd´s y revise la bahía de disquetes de la computadora y márquela para evidencia.
- Coloque disquetes formateados o cd´s en blanco en las bahías de la computadora.
- Proteja las entradas de las bahías con cinta.
- Pregunte al sospechoso o trate de averiguar si hay claves de acceso bien sea sobre información de la familia, mascotas, hobbies, que pueden ofrecer pistas para identificar las claves de acceso (passwords)
- Busque en toda el área claves de acceso escondidas, por ejemplo, debajo del asiento, en agendas de escritorio, notas pegadas, etc., y de encontrarlas protéjalas como evidencia.
- Asegure todos los manuales, documentación existente, disquetes y software.
- Asegure todas las notas diversas, papeles y registros escritos.
- Fotografíe cualquier equipo que parezca dañado.
- Registre el modelo y números de serie de todo el equipo que deberá ser asegurado.
- Inventaríe y etiquete cada pieza de evidencia.
- Marque toda la evidencia para ser empacada en cajas e identifíquelas.
- Fotografíe el equipo que será empacado antes de ser guardado en cajas.
- Cuidadosamente empaque el equipo en cajas con adecuadas envolturas, preferentemente antiestáticas.
- Ate todos los cables y líneas de comunicación.
- Tenga mucho cuidado con los pines de los conectores.

- Etiquete cada caja con el equipo dentro.
- Tome fotos del lugar de los hechos antes de retirarse.

Transporte

- Transporte todas las cajas (evidencia), de una manera cuidadosa.
- No transporte equipo de cómputo cerca de equipo de radio.

Almacenamiento

- Almacene el equipo dentro de un área limpia, preferentemente con una temperatura regulada.
- No permita a ninguna persona encender el equipo en custodia.
- Registre todas las etiquetas describiendo los detalles en un archivo del caso.
- Disponga que el equipo esté listo para cuando lo requieran los especialistas técnicos en informática forense.
- Proporcione al área indicada un reporte del incidente, la petición de aseguramiento, (aplicable al ámbito policial), una descripción del tipo de evidencia que se tiene, por ejemplo, pornografía infantil, correos electrónicos amenazantes, registros financieros, etc.
- Una relación de palabras o nombres que deben buscarse dentro del disco duro.

Conclusiones

En la medida que crece y se diversifica el uso de sistemas informáticos, se incrementan también los riesgos de que los equipos de cómputo y dispositivos electrónicos, conectados o no a Internet, sean vulnerables a ataques o incidentes que ponen en peligro la confidencialidad, integridad y disponibilidad de los datos que en ellos se procesa, almacena o transfiere.

De allí la importancia fundamental de contar con programas preventivos, estrategias correctivas planes de emergencia y respuestas inmediatas para proteger los equipos y sistemas, así como salvaguardar información y datos.

La computación forense es una disciplina muy amplia. Aquí hemos abordado esencialmente la importancia que tiene un buen aseguramiento de la evidencia física y digital, así como la protección del lugar de los hechos.

Sin embargo, para profundizar en el análisis particular de la evidencia digital se hace necesario aplicar metodologías y técnicas para efectuar un proceso forense específico que cubre al menos cuatro pasos de acuerdo a los especialistas avanzados: Identificación de la evidencia; Preservación de la evidencia; Análisis de la evidencia; Presentación de la evidencia.

Si a todo lo anterior se complementan las mejores prácticas en materia de la auditoria y control interno, investigación corporativa y de análisis de inteligencia, sin duda, el tratamiento de los crímenes cibernéticos sería indiscutiblemente integral y muy efectivo.

3. "PHISHING SCAM" Nueva modalidad de delito cibernético

Desde hace aproximadamente año y medio ha proliferado una nueva forma de estafa y engaño por Internet, mediante el correo electrónico, dirigida al usuario final la cual proviene, por lo general, de una supuesta dirección de correo electrónico conocida y solicita actualización de datos de un banco, una tienda en línea, una institución reconocida (universidad, empresa de empleos, etc.), además de datos confidenciales.

Esta técnica, conocida como Phishing Scam, está basada en la ingeniería social y usa métodos tradicionales para generar confianza en el usuario final y mediante una institución de prestigio, obtener datos críticos y confidenciales.

A través de páginas Web que cumplen con reproducciones de los sitios reconocidos existentes (desde el logo de la corporación y toda la interfaz, pasando por ligas válidas a los portales de las empresas a estafar), Phishing genera mensajes de correo electrónico (e-mail) con la finalidad de engañar a los usuarios, obtener datos personales, datos financieros, o una simple contraseña.

Un poco de historia

La palabra Phihsing se basa en una analogía: los estafadores de Internet usan pequeños anzuelos por conducto del correo electrónico para "pescar" las contraseñas y los datos financieros de los usuarios del Internet. Este término fue acuñado alrededor de 1996 por los hackers que robaban las cuentas de acceso a usuarios de la compañía America Online (AOL).

La primera mención de Phishing en el Internet se da en el sitio de noticias underground alt.2600 en enero de 1996, no obstante, el término pudo haberse utilizado anteriormente en la edición impresa del boletín de noticias "2600".

De igual forma, el término Phishing se encuentra relacionado con el denominado Phreaking, acuñado en la década de los 60', para hacer referencia a los intrusos y espías telefónicos.

Cómo funciona

Por lo general, los estafadores crean este tipo de engaños con la finalidad de utilizar los datos recolectados y ejecutar transferencias de alto valor o, inclusive, montar esquemas sofisticados de suplantación de identidad, engaños y fraudes haciendo uso de la tarjeta de crédito.

De forma típica, un correo electrónico Phishing llega con la dirección y logo original de la compañía a través de una dirección de correo electrónico (también falsa, valiéndose de la suplantación de identidad del emisor), y solicita al destinatario del correo enlazarse a una página que simula y parece ser de una institución genuina, sin embargo, mediante ésta se redireccionará a un tercer sitio con el número y contraseña e cuenta del usuario, que son los datos que les interesan a los estafadores.

Si el correo electrónico es exitoso, los estafadores tendrán datos, desde el nombre del usuario estafado pasando por la huella del equipo que actualizó la información (dirección IP, dirección de correo electrónico, etc.), hasta el número de sus contraseñas y de tarjetas de crédito. Hasta este momento, se ha proporcionado simple y sencillamente información, datos que podrán ser utilizados para suplantar la identidad (crédito, identidad de persona, número de seguro social, número telefónico privado, dirección postal, etc.), inclusive, para venderlos a través e bases de datos especializadas para el envío de correo masivo (spam).

Esta situación no termina con el engaño, debido a que se suman los problemas de los principales fabricantes, primordialmente en aplicaciones utilizadas por los usuarios para navegar en Internet como lo es el caso de Fallas críticas en el Internet Explorer (Boletín de Seguridad UNAM-CERT 2005-015 "Vulnerabilidades críticas en MS Windows" –30 Julio 2004), donde la navegación le permite al intruso incrustar código malicioso en todos los clientes, haciendo más fácil este tipo de ataques. Este hecho fue dado a conocer el 10 de diciembre el 2003 y fue solucionado por el fabricante ocho meses después. Los ataques Phishing Scam crecen a ritmo acelerado, recientemente, Citigroup, Ebay, Paypal, Yahoo y Bank of America han sido víctimas de esta situación donde se engaña a usuarios con cuentas válidas en sus sistemas y día con día el número de reportes y compañías involucradas aumenta, conforme los usuarios reportan movimientos y saldos no válidos en sus cuentas.

Es importante señalar que aunque las firmas de servicios financieros han sido blancos iniciales de este tipo de engaños, hoy en día este fenómeno ha proliferado hasta en tareas comunes como la obtención de una simple cuenta de Internet, simulando ampliación de espacio en la cuenta de correo, hasta las famosas cuentas de 1 GB de espacio de información que actualmente todos buscan y se subasta en los sitios tradicionales de trueque y negociación por Internet y desean el espacio "gratis" sin considerar las consecuencias implícitas que trae el adquirirlas.

Posibles soluciones

Es difícil precisar una receta para la prevención de este tipo de ataques tan elaborados y sofisticados que suceden día con día, sin embargo, entre las constantes que se deben promover se encuentran: la información y capacitación de los usuarios de las distintas organizaciones.

Desafortunadamente, son pocas las organizaciones que dedican parte de sus esfuerzos a las campañas internas y cursos de actualización, lo que trae consigo el no estar preparados frente a este tipo de eventos, ni establecer normas y procedimientos que les ayuden a reaccionar y responder de forma apropiada ante incidentes de seguridad de este tipo.

Otras posibles soluciones incluyen el fortalecimiento de las bases de la seguridad informática que incluyen la detección, prevención y educación.

Para fomentar la cultura de la prevención y detección en el área de informática se creó el AntiPhishing Working Group (APWG), organismo que conglomera esfuerzos de diversas compañías, con la finalidad de documentar, informar y catalogar las distintas formas que emplean los intrusos mediante la técnica del Phishing Scam.

El APWG realizó una lista con las entidades bancarias online y los sitios de compras en donde se detectan más fraudes de este tipo. Citibank figura en primer lugar como el banco donde más víctimas se han registrado o cuyo nombre es utilizado con mayor frecuencia para hacer estafas.

En lo que va de este año se han registrado cerca de cuatro mil 500 ataques de Phishing Scam, y realmente resulta preocupante que semana tras semana el número de estafas aumenta. En junio de este año, se registraron mil 422 casos y se calcula que para finales de 2004 la cifra se duplicará. Hay que señalar que la mayoría de estos ataques ocurren en Estados Unidos en donde, según la compañía consultora especializada Gartner, se han generado pérdidas totales pro dos mil 400 millones de dólares a cada víctima.

(J. Carlos. Guel. CERT-UNAM. México)

4. Herramientas Forenses

La computación forense es una de las actividades profesionales de muy rápido crecimiento en el siglo XXI. El incremento vertiginoso de usuarios de Internet en combinación con la automatización constante de los procesos de negocio ha creado nuevas oportunidades para los ciber criminales. Según estimaciones de John R. Vacca, autor de la obra "Computer Forensics: Computer Crime Scene Investigation", se requieren por lo menos 50,000 especialistas en cómputo forense para poder combatir con efectividad las amenazas globales de ataques informáticos.

- La computación forense involucra la identificación, preservación, extracción, análisis y documentación de evidencia digital almacenada en diversos medios magnéticos para poder comprobar conductas ilícitas que incriminen sin ninguna duda a personas sospechosas de haber cometido un delito relacionado con recursos computacionales. La parte fascinante de esta disciplina científica es entender que la evidencia digital a menudo es creada por el sistema operativo de la computadora sin el conocimiento del usuario del equipo. La información se encuentra oculta en las entrañas de la máquina y para identificarla se necesitan de técnicas y herramientas de cómputo forense.

- Dado que las computadoras han llegado a ser prácticamente indispensables en muchas organizaciones, los propietarios o dueños de empresas deben proteger y resguardar adecuadamente la información critica. Una preocupación creciente hoy día es la posibilidad de que se dañen o destruyan los datos bien sea de manera accidental, negligentemente o por intenciones dolosas. En tal sentido, antes de que una persona sea informada que será despedida, un especialista en cómputo forense debería acudir al lugar de trabajo y crear un duplicado exacto de la información almacenada en la computadora de esa persona. De esta forma, en caso de que el empleado haga algún daño antes de dejar la empresa, el dueño de la misma quedaría mejor protegido. Tanto las acciones de daño como los datos destruidos pueden ser recuperados y convertirse en evidencia digital para reconstruir los pasos ejecutados por un empleado resentido y en consecuencia tener elementos para iniciar acciones judiciales.

- ¿Por qué existe la computación forense? Una vasta mayoría de documentos actualmente existen en forma electrónica. Digamos que ninguna investigación criminal que implica la revisión de documentos electrónicos estaría completa sin la aplicación del análisis forense para preservar evidencia. La computación forense asegura la preservación y autenticación de datos digitales, los cuales son por naturaleza frágiles y volátiles, y pueden ser alterados o borrados. También las técnicas forenses computacionales facilitan la recuperación de archivos eliminados y otras formas de información normalmente no visible a los usuarios.

- Independientemente de la causa de la pérdida de datos, un especialista en cómputo forense normalmente podría recuperar la información entre un 80 y 85% de las veces en un tiempo de entre 3 y 5 días. Por supuesto que estos números varían en determinadas circunstancias, además, hay casos en donde el daño es tan severo que la recuperación de datos no es posible.

- John Vacca destaca en su obra que los ataques terroristas no están acotados a los edificios emblemáticos ni a los aeropuertos. El uso de computadoras personales como “armas” en manos de delincuentes, algunos de tan sólo 16 años de edad, han causado pérdidas severas a través de Internet hacia agencias de gobierno, bancos, grandes corporativos, pequeñas empresas, etc.

La obra de John Vacca es un documento excelente para comenzar a adquirir los conocimientos necesarios e incursionar en esta nueva carrera. Está dirigido tanto a oficiales de cuerpos policíacos que cuentan con unidades de combate a los delitos cibernéticos como a especialistas en prevención y seguridad de la información.

5. Recomendaciones para el uso de los Servicios Bancarios por Internet (www.condusef.gob.mx)

El uso de la Banca por Internet ofrece ventajas en cuanto a facilidad, comodidad, y rapidez para el acceso a los servicios bancarios; sin embargo, a pesar de que las Instituciones Financieras han realizado considerables esfuerzos e inversiones para procurar las mejores condiciones de seguridad, el uso inadecuado podría incrementar la materialización de diversos riesgos, por lo que existen algunos aspectos que, si son tomados en consideración por el público usuario, aseguran un uso confiable del servicio de Banca por Internet:

a) Uso del equipo de cómputo utilizado para realizar transacciones financieras
b) Identificadores y Contraseñas
c) Cuidados durante el uso del servicio
d) Cuidado de su información personal
e) Fraudes y prácticas inadecuadas
f) Sitios de interés

La Comisión Nacional Bancaria y de Valores, en ejercicio de sus facultades, supervisa de forma permanente, entre otros aspectos, el que las instituciones mantengan controles adecuados para el uso del servicio de Banca por Internet.

a) Uso del Equipo de cómputo utilizado para realizar transacciones financieras. Existen riesgos en el uso de los equipos de cómputo debido a que existen programas y dispositivos electrónicos que pueden sustraer o interceptar la información que se transmite y procesa, sin que el usuario lo pueda conocer y a su vez ser recuperada por terceras personas. Para disminuir estos riesgos, es importante tomar en cuenta lo siguiente:

    i) Procure no realizar transacciones financieras en computadoras de uso público o que no sean de su confianza. En caso de tener que hacer uso de este tipo de computadoras, le recomendamos que cambie su contraseña, a la brevedad, desde una computadora segura.

ii) Evite, en la medida de lo posible, acceder al servicio de banca por Internet mediante hipervínculos. Digite la dirección de la página Web de la institución financiera directamente en su navegador. En algunas ocasiones los hipervínculos redirigen a otro tipo de páginas apócrifas que pretenden hacerse pasar por instituciones financieras para dar mal uso a la información ingresada.

iii) Con el fin de mantener su computadora segura, actualícela con herramientas que le permitan detectar la ejecución de programas "maliciosos" tales como: *spyware*, *virus*, *adware,* entre otros, y que controlen las conexiones de entrada y salida (*firewalls* personales). Algunos de estos programas son proporcionados por el proveedor de su sistema operativo.

iv) No abra correos electrónicos sospechosos o de remitentes desconocidos. Elimínelos y por ningún motivo descargue los archivos adjuntos. Tampoco conteste ese tipo de correos.

b) Identificadores y Contraseñas. La clave de usuario y sus correspondientes contraseñas son, en muchos casos, el único medio para identificar a los usuarios de Banca por Internet, por lo que la administración de estos elementos se vuelve crítica debido a que si alguien los obtiene, puede asumir su identidad en el sistema y quedar facultado para realizar, en su nombre, todas las operaciones sobre sus cuentas registradas en su servicio de Banca por Internet, por lo que es importante tomar en cuenta lo siguiente:

i) En el caso de que el Banco le permita definir y configurar su identificador de usuario, considere:
   - No usar valores triviales, obvios o de fácil deducción por terceros.
   - Utilizar al menos ocho caracteres alfanuméricos.

ii) Recuerde que su contraseña lo autoriza como un usuario válido en el servicio de Banca por Internet, por lo que no debe prestarla o divulgarla a ninguna persona.

iii) Al definir su contraseña, recuerde que nadie más debe conocerla ni debe ser anotada, únicamente debe memorizarla, considerando las características siguientes:

- Una longitud mínima de ocho caracteres alfanuméricos.
- La combinación de minúsculas, mayúsculas, números y caracteres especiales.
- Evite el uso de valores triviales, obvios o de fácil deducción por terceros.
- Cambie su contraseña en forma periódica o inmediatamente cuando considere que ésta pudo haber sido comprometida.
- Si el banco le requiere definir una "pregunta secreta" o pista para recuperar su contraseña en caso de olvido, procure que ésta no contenga a la contraseña en sí y evite utilizar respuestas obvias o que puedan ser conocidas por terceras personas. De preferencia evite utilizar esta opción si le es posible.
- Si cuenta con el servicio de Banca por Internet en más de una institución, procure utilizar contraseñas diferentes en cada caso.

c) Cuidados durante el uso del servicio. El uso de la Banca por Internet puede realizarse de manera más segura si se mantienen cuidados mínimos durante la ejecución de transacciones y si se observa una debida vigilancia sobre los movimientos en sus cuentas:

i) No debe apartarse de su computadora cuando tenga abierta una sesión de Banca por Internet. En caso de requerirlo, debe dar por terminada la sesión a través de la opción "Cerrar" o "Salir". Verifique que efectivamente su sesión ha terminado y de preferencia cierre el navegador, y en caso de un equipo público, también la sesión del sistema operativo.

ii) Consulte y concilie periódicamente los saldos de sus cuentas contra los movimientos realizados y confirmados por usted, tal como lo haría con otras formas de operación, por ejemplo en el uso de cajeros automáticos.

iii) Revise periódicamente las cuentas registradas por usted para realizar traspasos a terceros en el mismo banco e interbancarios.

iv) Desactive las opciones de “recordar contraseñas” y “autocompletar” en su navegador.

d) Cuidado de su información personal. Su información personal es valiosa y puede ser utilizada por terceros con fines distintos a los lícitos. Procure mantener reservas respecto a la difusión de la misma. Considere los siguientes aspectos:

i) Las instituciones financieras no requerirán en ningún caso mediante correo electrónico actualizar información personal, identificadores de usuario y contraseñas. Recuerde que un correo electrónico no es un medio seguro para el envío de información sensible. En caso de sospecha, consulte con su Banco sobre la autenticidad de los comunicados recibidos por cualquier medio.
ii) Verifique que el sitio corresponde al de su Banco. Existe una práctica fraudulenta que consiste en “clonar” páginas de bancos copiando su identidad gráfica con el fin de obtener identificadores y contraseñas de usuarios. Es importante que digite la dirección de la página Web de su banco en vez de utilizar ligas o hipervínculos desde otras páginas.
iii) Mantenga disponible la información para contactar los servicios de soporte técnico y de aclaraciones relacionados con la banca por Internet de su Institución Financiera.
iv) Si no requiere el uso de Banca por Internet, acuda a su Banco para cancelar por escrito dicho servicio.
v) Si cree que alguien está intentando cometer un fraude haciéndose pasar indebidamente por otra persona o como su Banco, comuníquelo a través de los canales de atención que su Banco tenga designados.

e) Fraudes y prácticas inadecuadas en el uso de Internet. Algunas de las siguientes son prácticas que derivan frecuentemente en fraudes a través de Internet.

i) **Phishing.** El término se asemeja al inglés "fishing" (pescando). Se llama así a la práctica fraudulenta de conseguir información confidencial, enviando un correo electrónico haciéndose pasar por una institución o agencia de gobierno con el propósito de que los receptores lo contesten o lo reenvíen con información real. Estos correos se transmiten en forma masiva esperando que algunos los contesten haciendo creer al público, que se está comunicando con su institución financiera y entreguen, en realidad, a los defraudadores información confidencial tal como clave de usuario, número de cliente, números de cuentas, password o PIN. Utilizan frases como “estamos actualizando nuestros registros”, “seguridad y mantenimiento”, “investigación de irregularidades”, “personalización de cuentas”, “su cuenta ha sido congelada”, “tenemos que reconfirmar sus datos”, “su tarjeta de crédito ha sido cancelada”, “usted tiene una suma grande de dinero en su cuenta, por favor verifique sus movimientos”, “actualice sus datos”. Lo anterior, es para lograr convencerlo de proporcionar sus datos.

ii) **Keyloggers.** Son dispositivos físicos (conectados entre la PC y el teclado) y programas que se instalan en las computadoras que tienen como fin almacenar en un archivo todo el texto que se digita en un teclado. Posteriormente, este archivo es recuperado con el fin de conocer toda la información que el usuario digitó, incluyendo sus identificadores de usuario y contraseñas. El riesgo es mayor si utiliza equipos públicos de Internet (cafés Internet, hoteles, de otro usuario) o si alguien más tiene acceso físico a su computadora.

iii) **Web Page Spoofing.** Consiste en crear un sitio Web con dirección y apariencia similar al de una institución o empresa con el fin de obtener mediante los campos “normales” para capturar sus datos personales, la información de clientes. Al creer que se está en la página real de la institución, el cliente proporciona su nombre de usuario y contraseña. Por lo general, es más fácil confundirse con estas páginas al acceder a ellas mediante ligas colocadas en páginas de “concentradores de información” o de terceros en general.

iv) **Spyware.** Es un tipo de programas o software que envía su información personal sin su autorización y conocimiento a terceros. El tipo de información que se envía comprende los sitios Web visitados, nombres de usuario, contraseñas. La información puede ser utilizada para hacer mal uso de ella, y en algunos casos para enviarle publicidad. Generalmente este programa se carga en las computadoras al abrir o "bajar" de Internet programas de distribución ilegal o de uso gratuito.

v) **Adware.** Es el software que muestra publicidad en su equipo. Se trata de anuncios que aparecen de repente en su pantalla en ventanas emergentes ("pop ups" o "banners"). El riesgo de este tipo de programas reside en que en ocasiones incluyen software *Spyware* sin ser de conocimiento de quien lo instala. Tanto el *Adware* como el *Spyware* se instalan sin permiso en su equipo engañándolo con botones que dicen realizar alguna función (descarga de juegos, premios, videos gratis o programas) o bien pueden incluirse en programas para compartir archivos en Internet. Muchos programas gratuitos disponibles en Internet incluyen *Adware* y *Spyware*.

vi) **Virus.** Son programas que se instalan en su computadora y que realizan tareas orientadas a la pérdida de información o uso inadecuado de los recursos de su computadora. Estos programas pueden venir adjuntos a archivos ejecutables, juegos, imágenes, scripts de páginas web, e instalarse sin que usted se dé cuenta hasta que se ejecuten y causen daño o pérdida de información. Pueden reproducirse y transmitirse en varias computadoras mediante correos, juegos y archivos ejecutables en general. Una variante son los denominados Gusanos ("Worms") los cuales no tienen la capacidad de reproducirse o los Caballos de Troya que se adjuntan en archivos válidos y esperan un tiempo o acción definida para activarse.

vii) **"Secuestro" de sesión**. Cuando usted trabaja en una computadora conectada a red ya sea en su trabajo o en lugares públicos, el administrador de ésta puede habilitar funcionalidad en su equipo para permitir "tomar el control" de su sesión o bien, monitorear su sesión, con lo que puede observar en su pantalla lo mismo que usted en la suya. De este modo puede hacerse de información valiosa que usted ingresa en las aplicaciones, páginas Web y correos.

En caso de que sea víctima de un fraude a través de Internet, contacte de forma inmediata a su Banco; en caso de ser necesario acuda a la unidad de Policía Cibernética de la PFP.

f) Sitios de interés

- www.seguridad.unam.mx
- www.cert.org.mx/main.dsc
- www.ssp.gob.mx
- www.condusef.gob.mx
- www.microsoft.com/latam/technet/seguridad/

Recomendación de la Comisión Nacional de Defensa de Usuarios de Servicios Financieros (CONDUSEF), enviada a Autoridades en México desde el 2003.

Operaciones financieras efectuadas a través de medios electrónicos.

Es notorio el auge que ha tenido la celebración de operaciones financieras a través de medios electrónicos, en donde es muy difícil percatarse de la seriedad de la empresa que se encuentra detrás de tal situación. La CONDUSEF, preocupada por estos eventos emitió una Recomendación a la Autoridad competente tendiente a enfatizar la importancia de que se reglamente de manera adecuada la celebración de operaciones y la prestación de servicios con el público, mediante el uso de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y de redes de telecomunicaciones.

Esta propuesta involucra establecer la posibilidad de que se expidan a favor del Usuario comprobantes con valor probatorio pleno; que se refuerce mediante los Contratos de Adhesión el uso de claves de identificación y confirmación adicionales al Número de Identificación Personal (NIP); que se establezcan en los contratos de adhesión términos equitativos para la prestación de servicios a través de estos medios; asimismo, se sugirió a la Autoridad la investigación de las sociedades y portales informáticos con contenidos financieros o comerciales, cuyas operaciones son confusas y poco claras respecto del alcance legal y financiero.

Síntesis Curricular

Carlos Ramírez Acosta

Estudió en el Instituto Nacional de Ciencias Penales de la Ciudad de México. Es Criminólogo y Criminalista. Trabajó para el Banco Nacional de México por más de 20 años en el área corporativa de seguridad hasta el año 2000. Es miembro del Grupo Delitos Cibernéticos México, dependiente de la Policía Federal Preventiva. Ostenta el grado de Certified Protection Professional (CPP) en ASIS International, así como el grado de Certified Protection Officer (CPO) de la International Foundation for Protection Officers, IFPO, Capítulo México y Latinoamérica. Es socio fundador de la Federación Panamericana de Seguridad Privada (FEPASEP México); miembro de la Asociación Latinoamericana de Profesionales en Seguridad Informática (ALAPSI), y fue presidente de la mesa directiva de la International Association of Financial Crimes Investigators (IAFCI) y secretario de la International Association of Law Enforcement Intelligence Analysts (IALEIA), cargos ocupados en los capítulos mexicanos. Fungió también como secretario técnico del presidente del comité de comunicación y control sobre riesgos de lavado de dinero en Banamex. Tiene una amplia experiencia en seguridad, protección e inteligencia. Supervisó investigaciones corporativas cuyas afectaciones se produjeron por medios informáticos en productos y servicios bancarios. Ha sido un intenso promotor de la seguridad de la información y de la computación forense. Su especialidad está orientada al análisis de inteligencia, protección de información sensible y hacia la prevención e investigación criminal. La consultoría, la docencia y el trabajo en campo han sido sus actividades en los últimos 5 años llevando a cabo diversos seminarios de sus especialidades en México y América Latina. De entre varios diplomados universitarios, es egresado de la primera generación de Seguridad Informática de la Universidad Iberoamericana de México y del diplomado en Seguridad Nacional por el Instituto Nacional de Administración Pública. En el 2000, participó en un programa de entrenamiento en Análisis de Inteligencia Criminal en West Yorkshire Police Centre al norte de Inglaterra. Actualmente dirige su propia firma consultora denominada PRISMA Consulting Services.