Universidad Latinoamericana de Ciencia y Tecnología

ULACIT

Facultad de Ingeniería

Escuela de Ingeniería Informática

Trabajo final para optar por el titulo de licenciado en informática con énfasis en gestión tecnológica

Tema: Delincuencia Informática

Sustentante: Carlos Mejía Chacón

Cédula: 1-1126 0673

Tutor: Miguel Pérez

I Cuatrimestre 2007

Índice

Introducción

Como muchas de las invenciones productivas que cotidianamente son utilizadas, lamentablemente en sus inicios, Internet nace como una invención con fines militares financiado por el Departamento de Defensa de los Estados Unidos, algunas personas especulan que inclusive se desarrollaba esta red de redes por motivos de seguridad y comunicación ante un posible ataque nuclear. DARPA siglas en inglés de Defense Advanced Research Projects Agency fue la responsable directa del desarrollo de estas redes entre computadoras.

Posteriormente a esto se inicia la investigación en universidades norteamericanas y el proyecto de DARPA se torna una herramienta con fines educativos para el intercambio de información y conocimiento; cambia de nombre a ARPANET. ARPANET se convierte en el núcleo de lo que hoy se conoce como Internet.

En 1989 en Ginebra un grupo de físicos crea el lenguaje html basado en el SGML. En 1990 el mismo equipo construyo el primer cliente Web llamado World Wide Web (WWW) y el primer servidor web.

A partir de esto se inicia una revolución en el área del trabajo, comercio, el ocio y el conocimiento.

Millones de personas tienen a su disposición información de cualquier lugar del mundo en tan solo segundos. Los límites geográficos y las distancias se desvanecen en cuanto a adquisición de información se refiere. Lo que habitualmente tomaba días o hasta meses en correspondencia tradicional hoy es accesible de manera instantánea gracias a Internet.

Pero como es de esperar un gran poder implica también una gran responsabilidad. Estas herramientas tecnológicas en la actualidad, mantienen el orden de cuentas bancarias, información personal, registros médicos, etc. Con las herramientas adecuadas esta información tan valiosa pueda ser

accesada y modificada por un intruso, es realmente entonces una espada de doble filo.

En este documento se pretende exponer algunas de las metodologías normalmente utilizadas con fines vandálicos o de delinquir y posibles soluciones a esta problemática, es más sencillo implementar un sistema preventivo si se conocen las probables amenazas. Así mismo se presenta la forma en que es castigado en nuestro país estos delitos y como en muchos casos se crean vacíos legales y contradicciones que permiten fácilmente salir "ileso" a cualquiera que cometa estos cybercrimenes.

Delincuencia Informática

Conceptos

Inicialmente es de importancia saber a que nos referimos cuando utilizamos el término de delincuencia informática por tanto se describe seguidamente cada concepto para una mejor comprensión.

Fraude, se puede definir como: un engaño, una acción contraria a la verdad o a la rectitud.

Así mismo delito, "es una acción antijurídica realizada por un ser humano, tipificado, culpable y sancionado por una pena." [1]

Un delito informático se podría definir entonces como: toda acción culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que por el contrario produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la victima y debe realizarse en el entorno informático y estar sancionado con una pena.

Existen diversos términos que se utilizan normalmente en países de habla inglesa para denotar delincuencia informática, en el siguiente cuadro se exponen las principales expresiones

[1] *Lanverde, Leonardo y Soto Joaquín, Delitos Informáticos Recuperado el 2 de Marzo de 2007,http://www.monografias.com/trabajos6/delin/delin.shtml*

Cuadro 1.0 Principales términos que denotan delincuencia informática ingles-español

Ingles	Español
Computer Crime	Delito Informático
Computer Fraud	Fraude Informático
Computer Abuse	Abuso Informático
Corporate Fraud	Fraude Corporativo
Management Fraud	Fraude de Dirección
Electronic Burglary	Robo Electrónico
Data Processing Crime	Delito de Proceso de Datos
Hacking	Intrusión en sistemas informáticos

[2]

Clasificación de delitos informáticos

Los delitos informáticos pueden clasificarse como instrumento o medio y como fin u objetivo.

Siendo un **instrumento o medio** se describen como cualquier conducta criminal que irá dirigida en contra de las computadoras accesorios o programas. El sujeto o autor del ilícito obtiene un beneficio perjudicando a un tercero.

Dentro de la clasificación de los delitos informáticos identificados como instrumentos se tienen los siguientes:

- Falsificación de documentos vía computarizada.
- Lectura, substracción o copiado de información confidencial.
- Modificación de datos tantos de entrada como de salida.

[2] *Chinchilla C, (2004): Delitos Informáticos: Elementos básicos para identificarlos y su aplicación, San José, Editorial: Farben Grupo Editorial Norma*

- Aprovechamiento indebido o violación de código fuente para penetrar a un sistema, insertando nuevas instrucciones a los programas existentes.
- Variación en cuanto al destino de pequeñas cantidades de dinero a una cuenta bancaria apócrifa (“simulada”), método conocido como la técnica de salami.
- Alimentar con instrucciones que interrumpen la lógica interna de los programas con el fin de obtener beneficios.
- Alteración en el funcionamiento de los sistemas, a través de virus.
- Intervención de las líneas de comunicación de datos o teleprocesos.

Como criterio de clasificación de delitos informáticos identificados en su función de **fin u objetivo** en la realización de conductas delictivas se tienen:

- Programación de instrucciones que producen un bloqueo total en los sistemas.
- Destrucciones de programas por cualquier medio.
- Lesión física contra la maquina o sus accesorios.

  Otras clasificaciones:
- Acceso no autorizado: uso ilegitimo de passwords y la entrada sin autorización a un sistema informático.
- Destrucción de datos.
- Transferencias de fondos: Transferencias de dinero entre cuentas sin la autorización del legítimo dueño del dinero a transferir.
- Spamming: Envió masivo de correos electrónicos en forma deliberada.

Sujetos que intervienen en la actividad criminal informatizada

Se encuentran en esencia dos sujetos que intervienen en la actividad criminal informatizada, el **sujeto activo**: no son delincuentes comunes; tienen características particulares poseen importantes conocimientos de informática y

ocupan lugares estratégicos en su trabajo normalmente desde donde se realizan las actividades delictivas.

Sujeto pasivo: Persona u entidad sobre la cual cae la conducta que realiza el sujeto activo. En la mayoría de los casos, cuando ha resultado económicamente perjudicado por la ejecución de delitos informáticos, no denuncia esta situación y permanece en silencio, para no hacer más gravosa su posición y evitar la perdida de confianza de sus clientes. Muchas veces resulta más ventajosa la pérdida económica sufrida que las posibles consecuencias del conocimiento, por parte de los clientes, del daño o la intrusión en los sistemas de información de la empresa.

Características comunes en los delitos informáticos

Los delitos informáticos requieren de medios informáticos para su existencia. Algunas características importantes de los delitos informáticos son la rapidez en tiempo y la facilidad de encubrir el hecho delictivo.

Tipos de delitos informáticos

Costa Rica a pesar del gran desarrollo informático que goza con respecto al resto de Centroamérica, presenta un lento crecimiento en la regulación de delitos informáticos, esto dificulta en gran medida la persecución y proceso de entrega ante la justicia de las personas que comenten perjurios de manera informatizada.

Se citan a continuación una descripción específica de conductas consideradas como delitos informáticos y que posiblemente de ser reconocidas por las autoridades puedan implicar sanciones para los sujetos que las cometan:

- **Manipulación en el ingreso de los datos:**

  El sujeto activo no posee conocimientos especializados en informática pero tiene el poder de ingresar datos para su posterior procesamiento.

- **Manipulación en el procesamiento de datos ingresados:**

  Corresponde a la forma en que el autor manipula los datos que contiene la computadora, es decir procesa dicha información.

La manipulación se puede hacer alterando los programas existentes en el sistema de computadora insertando o modificando código fuente, programas o rutinas.

- **Intromisión en las bases de datos**: La información almacenada en bases de datos de empresas o instituciones, en la mayoría de los casos, no debe estar disponible para la consulta de los clientes o el público en general es el caso de los archivos médicos, criminales y de bancos.
- **Ingeniería social**: es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Un ingeniero social usará comúnmente el teléfono o Internet (muy posiblemente mediante medios como el phising termino que se explicara con mas detalle adelante en este documento) para engañar a la gente y llevarla a revelar información sensible, o bien a violar las políticas de seguridad típicas. Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a confiar en su palabra, antes que aprovechar debilidades de seguridad en los sistemas informáticos. Generalmente se está de acuerdo en que “los usuarios son el eslabón débil” en seguridad, como se sabe las cadenas por mas resistentes que sean se fragmentan siempre por el eslabón mas débil si se tensan con la fuerza adecuada; éste es el principio por el que se rige la ingeniería social.

  Uno de los ingenieros sociales más famosos de los últimos tiempos es Kevin Mitnick[3]. Según su opinión, la ingeniería social se basa en estos cuatro principios:

*** Todos queremos ayudar.**

*** El primer movimiento es siempre de confianza hacia el otro.**

*** No nos gusta decir no.**

*** A todos nos gusta que nos alaben.**

[3]*Kevin Mitnick es uno de los crackers y Phreakers más famosos de los Estados Unidos. Su último arresto se produjo el 15 de febrero de 1995, tras ser acusado de entrar en algunas de las computadoras más "seguras" de EE.UU..*

- **Fraudes contra sistemas; daños o modificaciones de programas o datos computarizados:** Entre las conductas de esta descripción encontramos: el sabotaje informático, los virus, las rutinas cáncer las bombas lógicas, el acceso no autorizado a un sistema y la reproducción no autorizada de programas informáticos.
- **Sabotaje informático:** Consiste en borrar, adicionar o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.
- **Los virus:** Todo programa que pueda ingresar en un sistema a través de cualquiera de los métodos de acceso de información externa. Básicamente el virus en su procedimiento de trabajo se instala en la computadora, se reproduce y finalmente causa algún tipo de daño de manera lógica.
- **Gusanos:** Es un programa con identidad propia; el cual una vez abierto busca espacio libre en memoria interna de la computadora y se autograba ahí de manera repetitiva hasta que ocurra situaciones como el desbordamiento de memoria, en algunos casos estos programas son capaces de enviarse a si mismo a destinatarios de correo electrónico que se encuentren almacenados en la computadora anfitriona.
- **Rutinas cáncer:** Se conoce como rutinas cáncer al programa que posee instrucciones y comandos que producen una auto reproducción del llamado programa cáncer al estilo de células orgánicas alcanzadas por un tumor cancerigeno maligno. Si se extraen estas rutinas, pero se deja una sola, resulta suficiente para que siga reproduciéndose y expandiéndose.
- **Bombas lógicas o cronológicas:** Es un conjunto de instrucciones que actúan en determinada fecha o circunstancia, destruyendo datos de la computadora y distorsionando el funcionamiento del sistema o paralizándolo.
- **Acceso no autorizado a sistemas o servicios:** Puede darse por diversos motivos ejemplo de esto son los llamados hacker o piratas informáticos que en muchas ocasiones simplemente intenta buscar la manera de burlar la seguridad de un servidor o un cluster de

computadoras de manera remota. Estos ingresos no autorizados comprometen la integridad y la confidencialidad de los datos almacenados en estos sistemas.

- **Denial of services (DOS**): Esta técnica lo que busca es saturar el servidor con rutinas repetitivas. Como es de suponer después de recibir miles de solicitudes por segundo el sistema colapsa.
- **Phising:** Metodología conocida en nuestro país y que es probable haya tenido éxito. Lo que busca es suplantar páginas de Internet por ejemplo de alguna entidad bancaria por sitios con contenido que simula la página original. El problema radica en que estas páginas almacenan y envían información de usuarios reales que no notaron la diferencia, estos datos son utilizados por terceros como propios. Muy sencillo seria poder conseguir el usuario y la contraseña de un usuario con poco conocimiento técnico o simplemente una persona poca cuidadosa que no se fije en pequeños detalles como la seguridad inherente que debe existir en una pagina banca electrónica.
- **Reproducción no autorizada de programas informáticos:** Se ha llegado a clasificar como delito la reproducción no autorizada de programas informáticos - Piratería - y la han sometido ha sanciones penales debido a la violación de derechos de autor.
- **Hurto realizado mediante transacciones electrónicas de fondos**: Este tipo de robo se comete mediante la utilización de sistemas de transferencia electrónica de fondos, la victima no es conciente que una transferencia es realizada desde su cuenta hacia una cuenta foránea. Normalmente se da este problema cuando no se cumplen con las precauciones de seguridad necesarias; por ejemplo se deja ociosa o abierta una sesión en una página de “internet banking”, de esta manera no existe ningún impedimento para realizar la transacción, la pagina esta a entera disposición del usuario.

Clasificación de los piratas informáticos:

- **Hacker:** Persona por lo general con grandes destrezas en el área de la computación. Dedica gran parte de su tiempo tratando de acceder a

sistemas mediante la violación de pequeñas vulnerabilidades como la adquisición de usuarios y contraseñas. Son herramientas de uso cotidiano para estos sujetos la utilización de programas con lógica de "fuerza bruta" la función de estas aplicaciones es buscar todas las posibles combinaciones que puede presentar un sistema para la autorización de ingreso de un usuario existente. Como es de esperar un procesador con características "*dual cores*" o procesadores múltiples como los que existen actualmente en el mercado tienen la capacidad de realizar miles de operaciones matemáticas por segundos sin embargo el proceso de encontrar finalmente un usuario y/o contraseña valido puede durar días o semanas dependiendo de la complejidad y la longitud de dicha cadena de caracteres.

En nuestro país las conductas que son realizadas por los "hackers" no son penalizadas; en países como Alemania y España este tipo de intrusiones son castigadas con todo el peso de la ley.

- **Cracker:** Su objetivo primordial es burlar los sistemas de seguridad de programas que requieren una autorización para su instalación o una posible renovación de la licencia. Realiza acciones de piratería informática como la copia ilegal de programas informáticos, obviamente infringiendo los derechos de autor.
- **Phreaker:** Este tipo de delincuente intenta mediante artimañas ingresar a las redes telefónicas para obtener beneficios personales. Por ejemplo llamadas gratis de larga distancia.

Delitos de violación a la intimidad:

Toda persona tiene derecho a la privacidad, sin la intromisión, curiosidad, vigilancia o espionaje de nadie. La violación de la intimidad ocurre cuando se observa, escucha o registra hechos, palabras, escritos o imágenes, valiéndose de instrumentos procesos técnicos u otros medios.

En Costa Rica es posible en casos de violación del derecho a la intimidad, la opción de acudir a los tribunales y presentar un recurso de habeas data, que es básicamente el derecho que debe de garantizarse a todo ciudadano de que su

información personal no ira ha ser accesada por personas que desean curiosear o realizar en general algún tipo de acto delictivo.

Es de conocimiento particular la existencia de una base de datos de información personal masiva en Centroamérica; Datum (http://www.datum.com); toda esta información puede ser adquirida por una suma determinada de dinero y obviamente es una violación al derecho de privacidad de las personas pero como en muchas situaciones en las que se ven involucrada la utilización de los medios informáticos por falta de conocimientos técnicos o de desconocimiento en general se pasan por alto.

Una de las herramientas más utilizadas para estos fines son los “keyloggers” que en esencia son aplicaciones que registran toda la información que es digitada y desplegada en la computadora. Una vez que los datos son capturados y almacenados no solamente se comete el delito de violación a la intimidad, también a partir de esta información se puede realizar robos de identidad, transferencias electrónicas sin consentimiento, entre otras.

A continuación en este documento se demostrara la instalación y funcionamiento de este programa antes descrito; es decir la usurpación de información de manera remota y sin la autorización del usuario para acceder a estos datos. Aplicaciones de este tipo son abundantes en Internet y son sumamente sencillas de utilizar y de activar.

Se advierte al lector que la siguiente información es únicamente con fines educativos y que la utilización de estas metodologías constituye un delito, además de implicaciones judiciales se deben de tener en cuenta el profesionalismo y la ética que debe existir en un verdadero profesional informático.

Ejemplo practico de un sistema que puede ser utilizado con fines de espionaje: aplicación de monitoreo remoto Perfect Keylogger

Nombre del aplicativo: Perfect Keylogger V1.47

Función: Captura de información en una aplicación no evidente para el usuario. Si se desea, la información que es capturada puede ser enviada a un correo pop3 o bien a un servidor mediante el protocolo de transferencia de archivos ftp; Como lo indica el nombre un “keylogger” es una bitácora de todos los “keystrokes” o presiones realizadas al teclado de una computadora como función primordial. Además de esto el programa permite el envió de “screenshots” o capturas de pantallas de manera periódica.

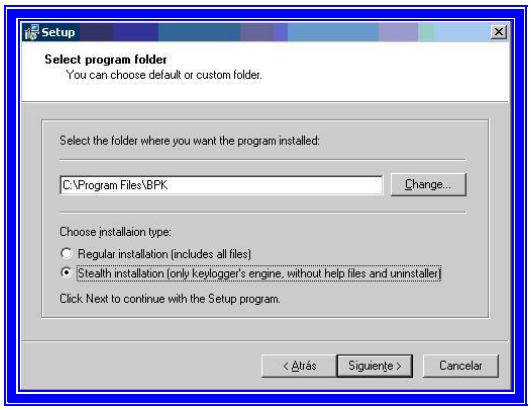


Figura 1.0: Proceso de instalación de la aplicación Perfect Keylogger

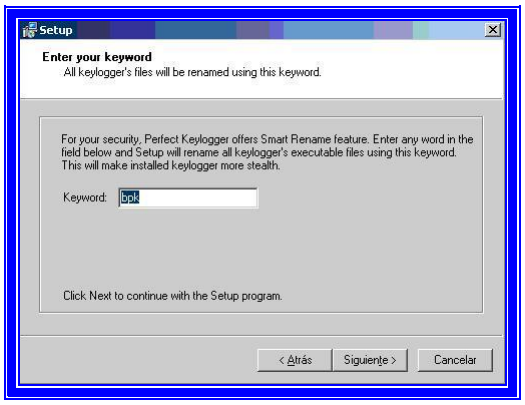


Figura 1.1 Instalación de Perfect Keylogger

Observamos como el asistente automático sugiere que sea cambiado el nombre del archivo ejecutable para no hacerlo evidente en el administrador de tareas del sistema operativo en este caso Windows Xp.

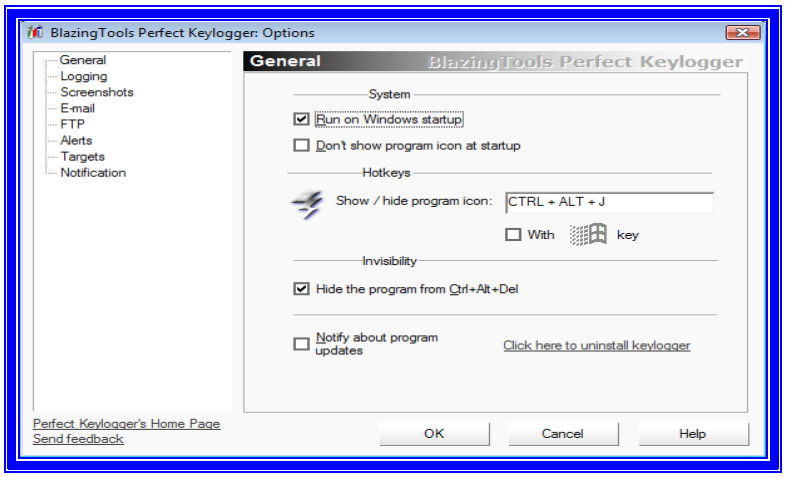


Figura 1.2: Opciones generales de perfect keylogger.

Una vez instalado es posible elegir opciones mediante “checkboxes” para ocultar y hacer menos accesible el programa de monitoreo en la computadora victima. También se debe elegir una combinación de teclas para activar el programa y hacerlo nuevamente evidente, de esta manera poder acceder a la información que ha sido capturada producto de la implantación. No necesariamente es requisito tener acceso a la computadora victima de manera fisica; también como se ha explicado en apartados anteriores la actividad del host puede ser monitoreada de manera remota.

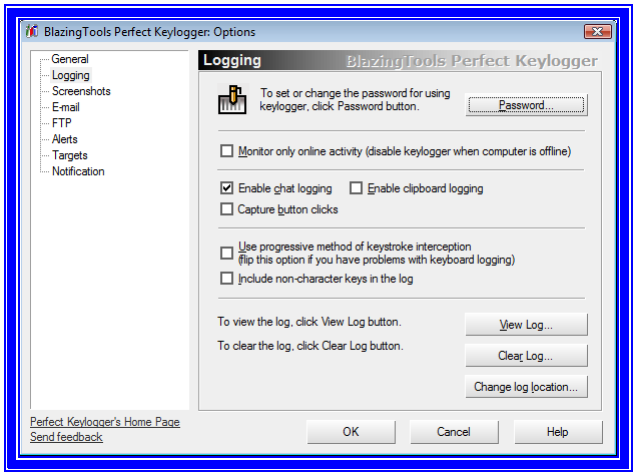


Figura 1.3: Opciones de bitácoras

Como es posible observar en esta sección del programa es factible ingresar un password para que únicamente la persona que implemento el sistema pueda leer las diferentes bitácoras.

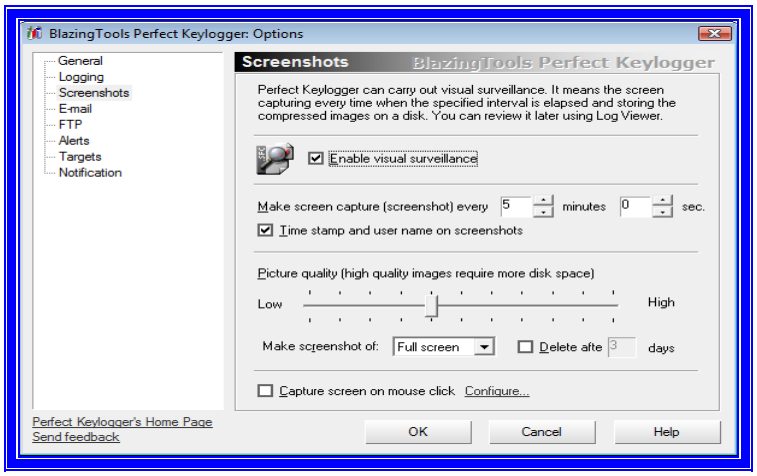
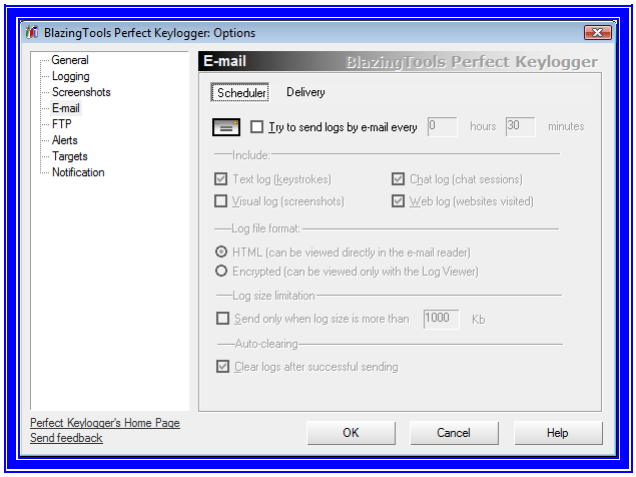


Figura 1.4: Captura de Screenshots

El programa permite habilitar opciones de vigilancia mediante capturas de pantallas, se puede escoger la calidad de las imágenes obviamente entre mayor sea la calidad de la imagen, mayor será el espacio que requerirá para almacenamiento. Se definen también los lapsos de tiempo en los que se desean realizar las capturas.



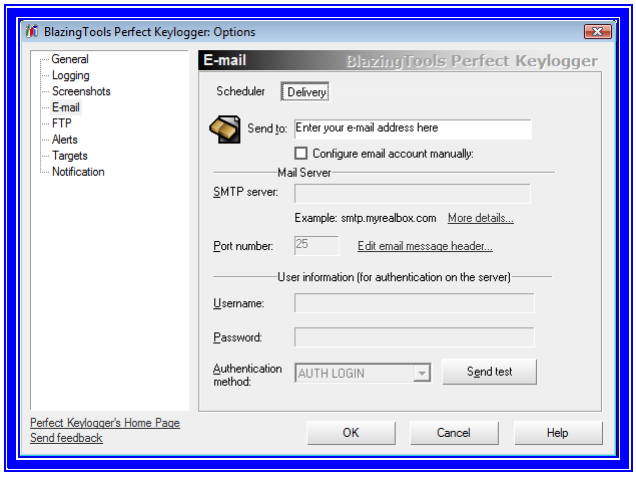


Figura 1.5: Envió de las bitácoras mediante E-mail

Se definen los intervalos de tiempo en los que se desean enviar las diferentes bitácoras a determinada dirección de correo. Se debe utilizar un correo pop3 de lo contrario la aplicación no funcionara.

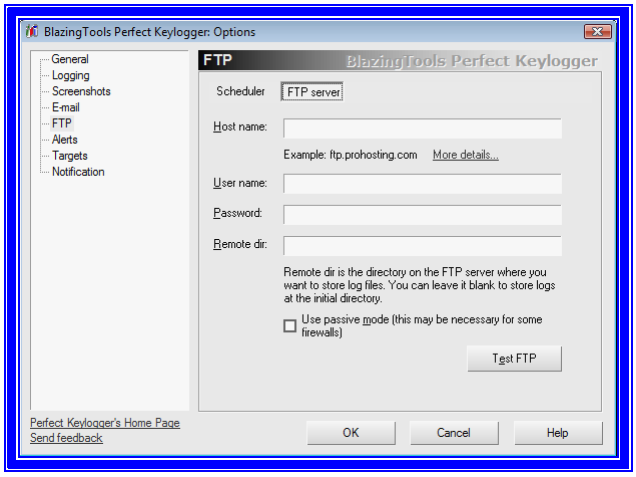


Figura 1.6: Envió de bitácoras a un servidor

Se utiliza el protocolo de envió de archivos para si el usuario desea enviar las bitácoras a un servidor este es un procedimiento muy similar al que se utiliza para enviar la información por correo.

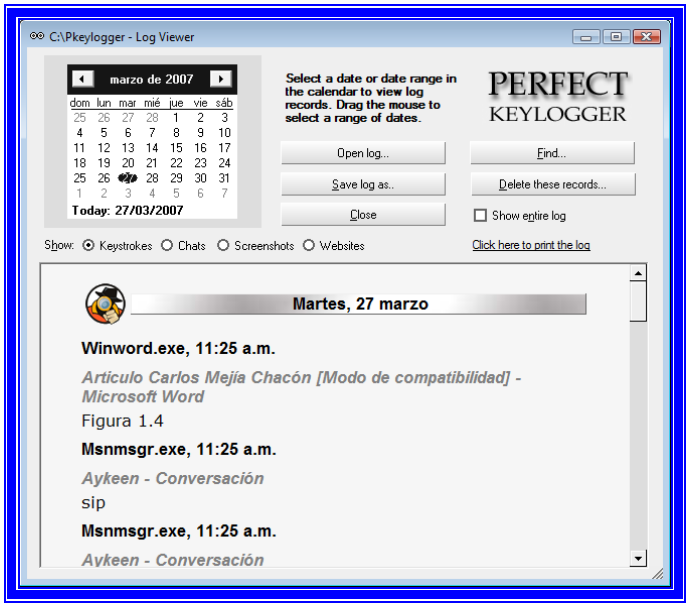


Figura 1.7: Bitácora

El programa registra las aplicaciones y los procesos que están en funcionamiento en el momento. La herramienta es tan eficiente que desencripta los caracteres con mascaras que se utilizan por ejemplo en aplicaciones web

como las que son utilizadas por los bancos para proteger el ingreso a esos sitios.

Además de todas estás funciones es posible enviar este programa utilizando una técnica de troyano. La aplicación se combina con un archivo ejecutable por ejemplo algo muy común un juego de flash o una presentación de power point y al abrir el programa se auto instala e inicia su funcionamiento. Funciona perfectamente.

Seguridad Informática

Aunque las aplicaciones para fines ilícitos son cada vez más sofisticadas y difíciles de detectar; lo que debe de imperar para la protección de todo sistema informático es la prevención. Toda actividad intrínsecamente asume riesgo, es por eso que lo óptimo es prepararse para ese riesgo antes que llegue a concretarse.

Para guardar un objeto de manera segura y prevenir una intromisión, es necesario lo siguiente:

- **La autenticación (promesa de identidad)**: es decir la prevención de suplantaciones, que se garantice que quien firma un mensaje es realmente quien dice ser.
- **La autorización:** se da permiso a una persona o grupo de personas de poder realizar ciertas funciones, al resto se le niega el permiso y se les sanciona si las realizan.
- **La privacidad o confidencialidad:** es el más obvio de los aspecto y se refiere a que la información solo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos. La transmisión a través de un medio presenta múltiples oportunidades para ser interceptada y copiada: la intercepción o recepción electromagnética no autorizada o la simple intrusión directa en los equipos donde la información está físicamente almacenada.
- **La integridad de datos:** La integridad se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de transmisión o en su propio equipo de origen.

Es un riesgo común que el atacante al no poder descifrar un paquete de información y, sabiendo que es importante, simplemente lo intercepte y lo borre.

- **La disponibilidad de la información:** se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.
- **No rechazo:** la protección contra alguien que niega que ellos originaron la comunicación o datos.
- **Controles de acceso:** esto es quien tiene autorización y quien no para acceder a una pieza de información determinada.

Medidas de seguridad de una red.

Existen numerosas técnicas para proteger la integridad de los sistemas. Lo primero que se debe hacer es diseñar una política de seguridad. En ella, definir quiénes tienen acceso a las diferentes partes de la red, poner protecciones con contraseñas adecuadas a todas las cuentas, y preocuparse de hacerlas cambiar periódicamente (Evitar las passwords "por defecto" o demasiado obvias).

Firewalls: Existen muchas y muy potentes herramientas de cara a la seguridad de una red informática. Una de las maneras drásticas de no tener invasores es la de poner “paredes”. Los mecanismos más usados para la protección de la red interna de otras externas son los firewalls o paredes de fuego. Estos tienen muchas aplicaciones, entre las más usadas está:

Packet filter (filtro de paquetes): Se basa en el tratamiento de los paquetes IP a los que aplica unas reglas de filtrado que le permiten discriminar el tráfico según indicaciones.

Normalmente se implementa mediante un router. Al tratar paquetes IP, los filtros que podremos establecer serán a nivel de direcciones IP, tanto fuente como destino. También es posible implementar una pared de fuego mediante software un ejemplo muy claro es el firewall que fue implementado por Microsoft en su nuevo sistema operativo Windows Vista.

Firma digital: El cifrado con clave pública permite generar firmas digitales que hacen posible certificar la procedencia de un mensaje o autenticar un determinado procedimiento que implique la utilización de medios informáticos, en otras palabras, asegurar que proviene de quien se dice. De esta forma se puede evitar que alguien suplante a un usuario y envíe mensajes falsos a otro usuario, por la imposibilidad de falsificar la firma. Además, garantizan la integridad del mensaje, es decir, que no ha sido alterado durante la transmisión. La firma se puede aplicar a un mensaje completo o puede ser algo añadido al mensaje.

Las firmas son especialmente útiles cuando la información debe atravesar redes sobre las que no se tiene control directo y, en consecuencia, no existe posibilidad de verificar de otra forma la procedencia de los mensajes.

Existen varios métodos para hacer uso de la firma digital, uno de ellos es el siguiente: “quien envía el mensaje lo codifica con su clave privada. Para descifrarlo, sólo puede hacerse con la clave pública correspondiente a dicha persona o institución. Si efectivamente con dicha clave se descifra es señal de que quien dice que envió el mensaje, realmente lo hizo”.

Política de seguridad: Proveer acceso a los servicios de la red de una empresa y proveer acceso al mundo exterior a través de la organización, da al personal e institución muchos beneficios. Sin embargo, a mayor acceso que se provea, mayor es el peligro de que alguien explote lo que resulta del incremento de vulnerabilidad.

De hecho, cada vez que se añade un nuevo sistema, acceso de red o aplicación se agregan vulnerabilidades potenciales y aumenta la mayor dificultad y complejidad de la protección. Sin embargo, si se está dispuesto a enfrentar realmente los riesgos, es posible cosechar los beneficios de mayor acceso mientras se minimizan los obstáculos. Para lograr esto, se necesitará un plan complejo, así como los recursos para ejecutarlo.

También se debe tener un conocimiento detallado de los riesgos que pueden ocurrir en todos los lugares posibles, así como las medidas que pueden ser tomadas para protegerlos.

Después de todo, se le va a confiar a ellos los bienes más importantes de la organización.

Para asegurar una red adecuadamente, no solamente se necesita un profundo entendimiento de las características técnicas de los protocolos de red, sistemas operativos y aplicaciones que son accesadas, sino también lo concerniente al planeamiento. El plan es el primer paso y es la base para asegurar que todas las bases sean cubiertas.

Conclusiones:

A través de este documento se han descrito algunas metodologías de delitos informáticos existentes, y que pueden o han llegado ha cometerse en nuestro país. Como se ha expuesto nuestro sistema judicial todavía no concluye de manera óptima las penalizaciones sobre estas conductas que en realidad pueden traer consigo grandes perdidas económicas tanto a grandes empresas como a particulares.

Es de conocimiento general que la “expertise” requerida para cometer un ciberdelito es un factor primordial, sin embargo en Internet cada vez es mas frecuente encontrarnos con manuales paso a paso de cómo infiltrarse en sistemas y no se requiere de una curva de aprendizaje superior para poder dominar la utilización del programa y sus características.

Día a día podemos ir conociendo nuevas formas de delincuencia cibernética, la realidad camina un paso adelante que el sistema penal costarricense. No es posible dejar nuestra sociedad globalizada al servicio de los delincuentes informáticos, nuestra legislación debe actualizarse; la experiencia de otras

naciones resulta de gran relevancia para una futura implementación de castigos reales para personas que comentan errores de esta índole.

Debido a la naturaleza virtual de los delitos informáticos, puede volverse confusa la tipificación de éstos ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo en el area judicial. Desde el punto de vista de la Legislatura es difícil la clasificación de estos actos, por lo que la creación de instrumentos legales puede no tener los resultados esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las leyes relacionadas con la informática.

La ocurrencia de delitos informáticos en las organizaciones alrededor del mundo no debe en ningún momento impedir que éstas se beneficien de todo lo que proveen las tecnologías de información (comunicación remota, Interconectividad, comercio electrónico, etc.); sino por el contrario dicha situación debe plantear un reto a los profesionales de la informática, de manera que se realicen esfuerzos encaminados a robustecer los aspectos de seguridad, controles, integridad de la información, etc. en las organizaciones.

La investigación en sitios de discusión sobre seguridad informática, el cuidado del entorno como usuario y la mejoras en las arquitecturas de red que son realizadas satisfactoriamente son pasos a seguir si se desea realmente disminuir o minimizar la materialización de riesgos asociados a delitos informáticos. Sin embargo hay que estar consiente que para toda medida de seguridad siempre existirá una o muchas maneras vulnerabilidades, no importa la complejidad; el ingenio y la astucia en la mayoría de los casos se sobrepone a las grandes inversiones.

Bibliografía

Campoli, G. (2003) *Derecho Penal Informático.* San José: Investigaciones Jurídicas S.A.

Hess Araya, C. (2002) *La Dimensión Jurídica del Software: Naturaleza, tutela jurídica, contratos y responsabilidad.* San José: Investigaciones Jurídicas S.A.

Duncan-Lich, P , Jiménez Vargas, F , Rodríguez, JC (2001) *Código de propiedad intelectual.* San José: Investigaciones Jurídicas S.A.

Zuñiga Morales, U. (2000) *Código Penal.* San José: Investigaciones Jurídicas S.A.

Chinchilla C, (2004)*: Delitos Informáticos: Elementos básicos para identificarlos y su aplicación,* San José, Editorial: Farben Grupo Editorial Norma

Lanverde, Leonardo y Soto Joaquín*, Delitos Informáticos Recuperado el 2 de Marzo de 2007, http://www.monografias.com/trabajos6/delin/delin.shtml*

Anexos

Seguridad en Internet

WEB: SI LE PARECE QUE SU NEGOCIO ESTÁ BAJO UN ASEDIO ELECTRÓNICO CONSTANTE A TRAVÉS DE LA RED, LLEGÓ LA HORA DE INCREMENTAR SUS CONOCIMIENTOS DE PREVENCIÓN

Busque los contactos de estas empresas en la página 130

Por Amanda C. Kooser y Eric Bender

ALGO ACECHA EN SU BANDEJA DE ENTRADA. Un programa de guerra husmea por su red Wi-Fi. Ese adjunto del correo electrónico no trae buenas intenciones. Sus códigos de seguridad pueden resultar afectados. Los hackers ya consideran suyo su sitio en la Red. Algunas veces parece que su negocio está bajo un asedio constante a su seguridad. Bueno, ya es hora de dejar de preocuparse y adentrarse al tema de la seguridad en Internet. El conocimiento y la preparación son lo único que tiene para no perder

FOTOARTE: MARIO M. RAMOS

información, productividad y mucho dinero.

Si quiere saber sobre la biometría, tiene curiosidad acerca de la eficacia de los cortafuegos o sobre el espionaje de los empleados, entonces entérese de lo que están haciendo los expertos y los empresarios sobre estos y otros aspectos. Después de todo, cuando se trata de la seguridad en la red, la prevención significa tener ganada más de la mitad de la batalla.

> "El conocimiento y la preparación son lo único que tiene para no perder información, productividad y mucho dinero."

No más basura

El spam —correo electrónico no solicitado. Generalmente, contiene publicidad y promociones. También se le conoce como correo basura— no sólo es molesto, sino que cuesta dinero a su negocio. No es fácil cuantificarlo en pesos, pero todo ese tiempo que invierten usted y sus empleados para separar los correos útiles de los inútiles, añaden pérdidas a la productividad. La compañía investigadora de mercados y tecnología, Ferris Research Inc. calcula que el spam costó a las empresas estadounidenses más de 10 mil millones de dólares en 2003.

Paul Hodara, presidente y fundador de la compañía NetWave Technologies (www.netwave.com), proporciona servicios de Red a las empresas. Las demandas de sus clientes han llevado a NetWave, con oficinas centrales en Nueva York, a ofrecer una solución contra el spam: ellos son los que limpian de spam los servidores de correo electrónico de sus clientes. El consejo de Hodara para combatir el spam se inicia en una parte no necesariamente técnica: "Me gusta atender primero a las políticas antes de ocuparme del software. Me gusta que los empleados establezcan procedimientos de manera interna dentro de su organización". Sugiere que una política escrita incluya apartados como no responder a los correos del spam, no dar entrada a enlaces de opción externa y no registrar su domicilio de correo electrónico en sitios de la Red donde lo puedan encontrar y utilizar. Hay que asegurarse que todos los empleados tengan esas instrucciones.

Las oficinas centrales de las empresas y otros negocios que tengan unos cuantos usuarios del correo electrónico, pueden beneficiarse del software comercial como el SpamKiller de McAfee (www.mcafee.com) o el Norton AntiSpam de Symantec (www.symantec.com).

Cuando se trata de compañías grandes con sus propios servi-

dores de correo electrónico, se tiene que implantar ya sea una solución en el servidor como el InterScan VirusWall de Trend Micro (www.trendmicro.com) o dejar que se encarguen de ello compañías como NetWave.

Esto último implica beneficiarse de un cierto software sin tener que darle mantenimiento, lo cual es una bendición para los empresarios porque se evitan tener un personal de Tecnologías de la Información (TI) interno. Ya sea que se trate de una sola persona o de alguien con 100 empleados a su cargo, es el momento de recuperar los correos electrónicos propios y de recobrar el tiempo y la productividad. Porque según lo indican las investigaciones, el spam se pondrá peor.

E-transacciones seguras

Olvídese del atraco punto com. El comercio electrónico (e-commerce) se ve bastante saludable estos días. Los empresarios que inician su tienda virtual o que ya consideran agregar capacidades de e-commerce a un sitio ya existente, tendrán que aceptar, cada vez más, el pago mediante tarjetas de crédito.

Aunque los compradores por Internet son todavía más cautelosos que antes con respecto a la seguridad, los propietarios de negocios también lo deberían de ser. En 2002, el 47 por ciento de las quejas por fraude presentadas a Comisión Federal de Comercio estadounidense, se relacionó con ventas por Internet. Las subastas en línea constituyen la fuente más notoria de fraude, aunque las anomalías con tarjeta de crédito y de débito son un asunto aparte.

Algunos empresarios preferirán que alguien más se ocupe de manejar completamente sus transacciones con tarjeta de crédito. En los servicios como el de Yahoo!, las tiendas se encargarán de hacer ese trabajo por usted. Sólo hay que asegurar que su proveedor sea de reputación y cuente con las instalaciones técnicas debidas para realizar transacciones con tarjeta de crédito.

El sitio electrónico de servicios editoriales InkNoise, decidió utilizar los servicios del banco en línea denominado National Inter-Bank Banking Center (www.nationalin terbank.com) para el manejo de su cuenta de negocios, el "Charge.com" para el procesamiento y a GeoTrust (www.geotrust.com) para el certificado SSL (Secure Socket Layer) de capa de conexión segura. Este último paso tiene una importancia particular: la SSL es el sistema que codifica y asegura la precisión de los datos que envían a los clientes.

Diversificar entre distintas empresas las tareas que se derivan de tener la posibilidad de comercio electrónico en su sitio le resultará acertado toda vez que busque las mejores tarifas y proveedores por rubro.

De hecho, esta es una sugerencia indispensable para los empresarios menos conocedores de las TI: deje que los especialistas en códigos y administración de servidores se ocupen de esta labor.

Juegos de espías

Espionaje de empleados: suena como algo salido de las películas, y casi uno se puede imaginar a un empleado pendiendo de cuerdas y escabulliéndose de los rayos láser. La realidad no es tan sorprendente, pero sí peligrosa para su negocio.

Puede manifestarse en robos de listas de clientes o de información industrial, en robo de software, en fraudes con cheques de negocios o en sacar dinero por medio de los libros.

El primer punto que debe entenderse es que todo negocio puede estar en riesgo. No sólo resulta evidente que los empleados descontentos se vuelven un problema, sino también aquellos que enfrentan dificultades financieras o que piensan iniciar empresas rivales.

El detective Michael Terrell del Departamento de Policía de Omaha, Nebraska, ha investigado varios delitos en oficinas y fechorías cibernéticas. "Siempre preguntamos: '¿investigó los antecedentes o la historia delictiva del personal a contratar?' Si no hizo una investigación de antecedentes, entonces no sabe a quién le está dando trabajo", dice Terrell.

Una pequeña inversión inicial en tiempo le puede evitar una pérdida mayor en el futuro.

La protección de su negocio contra el espionaje de los empleados comienza con la preparación de una política y en su aplicación. Tanto en su manual como en los contratos de trabajo, asegúrese de incluir cláusulas que estipulen que todo el trabajo producido le pertenece a la compañía y no a los empleados.

"Si les asignará una labor delicada en la que tengan que manejar bases de datos de clientes o dinero, deberá haber un sistema de trabajo en pareja", Terrell así lo recomienda. "Una persona no puede tener el acceso a todo." A nivel de computadoras, los respaldos escrupulosos de su servidor y el empleo de códigos de seguridad pueden ayudarle a proteger sus datos.

> "Establezca internamente procedimientos en base a políticas en su organización. Después ponga su atención en el software."

Control de fallas

Con los asaltos de virus electrónicos como el Slammer y Blaster del año pasado, "las amenazas tienen sus cambios", dice Vincent Weafer, director general del grupo de Respuesta de Seguridad de Symantec.

Uno puede recibir un ataque directo por Internet o por correo

electrónico, de sitios de la Red, de la mensajería instantánea, desde un punto de acceso inalámbrico, por paquetes de nivel semejante, por carpetas de archivos compartidos y seguramente a través de algo diferente en el futuro.

"Si tiene un sistema que esté expuesto, automáticamente puede ser escaneado y atacado de 15 a 20 minutos después", agrega Weafer.

Cada vez más, las compañías pequeñas son el blanco de tales ataques. Y no se trata de que los hackers estén más interesados en sus clientes, sino debido a que "quieren usar su dirección de correo para atacar a otras personas", comenta Weafer. Lo que se necesita, dice, es "defenderse a profundidad".

Esto significa emplear una suite de herramientas que proteja tanto a las PCs individuales como a los recursos de red compartida, como son la compuerta de enlace a Internet o el servidor de mensajería. Weafer hace énfasis también en la necesidad de actualizar regularmente el software antivirus.

Además, se debe tener cuidado especial con las laptops y otras PCs remotas. "Se encuentran situaciones en que el 90 por ciento de las máquinas están bien protegidas, y luego se trae una laptop e infecta a toda la red", remarca Weafer.

Los creadores de antivirus han tomado medidas para responder más rápido ante las crisis importantes, anota David Perry, director general de instrucción de Trend Micro.

Sin embargo, el software antivirus no realiza todo el trabajo. También se necesita de un cortafuego apropiadamente configurado, parches de seguridad para Windows con implantación regular u otro software decisivo, códigos de seguridad que se apliquen y una política de seguridad de la compañía que entienda todo el mundo.

Otras herramientas de software que llegan por cuentagotas de las grandes compañías también demuestran ser sumamente deseables. Las que filtran contenidos no sólo bloquean el spam y el acceso a sitios inconvenientes de la Red, también revisan la información clave que entra o sale —asegurando que la información de tarjetas de crédito no salga por el correo electrónico, por ejemplo—. Estas alertan de cuando alguien intenta colarse o cuando algún programa está registrando ciertos tecleos, por ejemplo.

Además, se debe escanear el sistema para encontrar puntos débiles.

Existe un sistema central de herramientas automatizadas para realizar esta labor. Se pueden probar algunas gratis (como Qualys www.qualys.com), ya que los proveedores saben que la seguridad no es un asunto de una sola intervención.

Alternativamente, se puede acudir a un especialista en seguridad, en especial si se está en expansión o se van a hacer otros cambios importantes en la red.

Bienvenido al Banco Nacional de Costa Rica

Protéjase usted mismo

La Seguridad en Internet se centra en usted.

Internet ha modificado la manera de ver la vida. Pero el mundo virtual, tiene sus riesgos y sus amenazas. Muchas de las experiencias que hacen que Internet sea tan valioso en nuestras vidas diarias también requieren que divulguemos información sobre nosotros mismos.

El resultado de la divulgación de información puede ser un fastidio, como los correos no deseados de spam. O podría tratarse de algo muy serio, como un intento de utilizar incorrectamente su buen crédito o robarle dinero.

Protegerse a usted mismo en Internet significa manejar o eliminar las molestias, y luego cuidarse contra preocupaciones más serias como el robo de identidad. Así es cómo se logra:

Practique comportamientos en Internet que reduzcan su riesgo.

Preste atención a los engaños en el spam - e ignórelos. Los artistas del engaño en Internet están listos para tomar su dinero o robar su identidad. ¿Su herramienta principal? el Spam, entregado como e-mail, mensajes instantáneos (MI), e incluso tarjetas electrónicas.

Una estafa por medio de spam que es particularmente solapado se conoce como

Utilice claves de acceso sólidas, y manténgalas en secreto. Para proteger información personal importante, bloquee el acceso a su computadora y a sus cuentas utilizando claves de acceso sólidas. La mayoría de las claves de acceso son descifradas por programas de computadora, no por alguien que adivina su clave. La mejor defensa es elegir una clave de al menos ocho caracteres de longitud, e incluir algunos caracteres además de letras y números. Nunca comparta sus claves de acceso con nadie, ni siquiera con sus amigos.

Sea cuidadoso al descargar. Solamente descargue software de sitios Web en los que confíe. Sitios pornográficos y de celebridades, así como de música "gratis" y programas de intercambio de archivos de películas, pueden contener software indeseado, incluso Spyware.

Instale programas de intercambio de archivos con mucha cautela. Utilizar estos programas, también conocidos como Peer-to-Peer o P2P, puede dejar una puerta trasera abierta en su computadora cuando se encuentre conectada a Internet. No comparta archivos con desconocidos. Algunas personas comparten lo que dicen ser archivos de música o películas, pero en realidad se trata de pornografía, virus o Spyware.

Utilice tecnología para reducir los riesgos y esté alerta cuando sea apropiado.

Los proveedores de servicios de Internet, el software como programas y servicios de e-mail, y los navegadores Web mejoran día con día. En algunos casos, bloquean miles de millones de e-mails con SPAM cada día. Y las nuevas tecnologías que surgen pueden analizar y señalar estafas potenciales de Phishing, y luego brindar sugerencias sobre lo que se debe hacer.

¿Qué hacer si se mete en problemas?

Para reportar Phishing:

. Reenvíe el mensaje de e-mail a su proveedor de servicios de Internet (ISP).

. Reenvíe el spam a la empresa que está siendo suplantada. Es posible que tenga una dirección especial para reportar estos abusos - por ejemplo abuso@microsoft.com.

Si usted cree haber sido víctima de robo de identidad:

Hable con el departamento de seguridad o fraudes de todos sus bancos o instituciones financieras, así como empresas de tarjetas de crédito, de servicios públicos, proveedores de servicios de Internet y otros lugares donde usted utiliza regularmente su tarjeta de crédito.

Phishing y parece provenir de una empresa en la que usted confía o incluso su propia compañía (por ejemplo hacen una copia exacta de la página de su banco). El mensaje falso (la "carnada"), típicamente contiene un enlace (el "anzuelo") hacia una página web o ventana desplegable igualmente falsa donde se le pide que revele datos personales. Para combatir las estafas, preste atención, confíe en sus instintos y siga estos pasos:

. Borre el spam (correo electrónico, mensajería instantánea), sin abrirlo. Nunca responda.

. Busque señales de estafa. Mensajes alarmistas y amenazas de cierre de cuentas. Promesas de mucho dinero por nada o poco esfuerzo. Negocios que suenan demasiado buenos para ser verdad. Faltas de ortografía y errores gramaticales. Solicitud de información personal, amenazas de cierre de cuentas, solicitud de usuario y password, mensajes alarmistas.

. No comparta información personal confidencial en un e-mail o mensaje instantáneo. (Si una empresa de reputación parece estar pidiéndole información personal, podría tratarse de una estafa).

Respete los derechos de propiedad. Usted se arriesga a meterse en problemas legales - pagar multas o incluso ir a la cárcel - si utiliza materiales sujetos a derechos de reproducción sin el permiso del propietario legítimo.

Maneje su información personal cautelosamente

Siga estas pautas cuando deba compartir información confidencial en línea - por ejemplo cuando compra, cuando se une a un grupo o cuando abre una cuenta.

. Elija con cuidado los lugares donde conduce negocios en línea. Lea las declaraciones de privacidad antes de entregar ninguna información personal.

. Busque indicaciones de que el sitio Web protege los datos confidenciales. Busque https ("s" de seguro) en la dirección Web y un pequeño candado cerrado o una llave entera.

. Asegúrese de estar donde cree que está. Desafortunadamente, el candado (o la llave) pueden ser falsificados. Así que asegúrese de abrirlo presionando dos veces el botón del ratón encima del candado y asegúrese que el nombre en la dirección Web calce con el del certificado de seguridad; si el nombre es diferente, usted puede estar en un sitio falso.

. Bríndele seguimiento con una carta y guarde una copia.

Cuando abra nuevas cuentas de correo electrónico o servicios de internet:

. Evite el uso de claves de acceso simples como por ejemplo: nombres de hijos, esposa o mascotas, números de teléfono.

. Modifique las claves en todas sus cuentas en línea, empezando con las que se relacionan con información financiera.