Ataques y amenazas

1. Consejo de Seguridad Informática ST06-005

Acerca de los Amedrentadores por Internet (Cyberbullies)

Los amedrentadores ahora están tomando ventaja de la tecnología para intimidar u hostigar a sus víctimas. Tratar el tema del acoso por Internet puede ser difícil, pero hay pasos que usted puede tomar.

¿Qué es el acoso por Internet (cyberbullying)?

Con acoso por Internet se hace referencia a una práctica nueva y en aumento de usar la tecnología para acosar u hostigar a otra persona. Los amedrentadores (bullies) solían estar restringidos a métodos tales como intimidación física, por correo postal o por teléfono. Ahora, los desarrollos en los medios electrónicos ofrecen foros tales como el correo electrónico, mensaje instantáneo, páginas web, y fotos digitales para agregar al arsenal. Las computadoras, teléfonos celulares y los Asistentes Digitales Personales (PDA) son nuevas herramientas que pueden ser aplicadas a una práctica vieja.

Las formas de amedrentamiento por internet pueden variar en severidad desde rumores crueles o embarazosos hasta amenazas, hostigamiento o acoso. Puede afectar cualquier grupo de edad; sin embargo, los adolescentes y adultos jóvenes son las víctimas comunes y el acoso por internet es un problema creciente en los colegios.

¿Por qué el acoso por Internet se tornó en una problema serio?

El relativo anonimato de Internet es atractivo para los acosadores porque acrecienta la intimidación y hace que sea más difícil rastrear la actividad. Algunos acosadores encuentran más fácil ser viciosos porque no hay contacto personal. Lamentablemente, Internet y el correo electrónico también pueden incrementar la visibilidad de la actividad. La información o fotos publicadas online o enviadas en correos electrónicos masivos pueden alcanzar a una mayor audiencia y más rápidamente que los métodos más tradicionales ocasionando más daño a las víctimas. Y debido a la cantidad de información personal disponible online, los acosadores pueden elegir a sus víctimas arbitrariamente.

El acoso por Internet también puede indicar una tendencia hacia una conducta más seria. Mientras que el acoso siempre ha sido una realidad desafortunada, muchos acosadores crecen a partir de esto. El acoso por Internet no hace mucho que existe y no es tiempo suficiente para tener una experiencia sólida, pero hay evidencia de que puede ser una alerta temprana de una conducta más violenta.

¿Cómo se puede proteger a sí mismo?

- **Tener cuidado del lugar donde publica su información personal** – Limitando la cantidad de gente que tiene acceso a su información de contacto o detalles acerca de sus intereses, hábitos o empleo, usted reduce su exposición a los amedrentadores o acosadores que usted no conoce. Esto puede limitar su riesgo de pasar a ser una víctima y puede facilitar identificar al acosador si usted se convirtió en una víctima.
- **Evitar magnificar la situación** – Responder con hostilidad muy probablemente provocará a un acosador y magnificará la situación. Dependiendo de las circunstancias, considere ignorar el tema. A menudo los acosadores avanzan sobre la acción de sus víctimas. Otras opciones incluyen acciones más sutiles. Por ejemplo, si usted está recibiendo mensajes de correo electrónico no deseado, considere cambiar la dirección de su correo electrónico. Si el acosador no tiene acceso a la nueva dirección, el problema puede detenerse. Si usted continúa recibiendo mensajes en su nueva cuenta, puede tener un caso más fuerte para una acción legal.
- **Documentar la actividad** – Mantenga un registro de cualquier actividad online (correo electrónicos, páginas web, mensajes instantáneos, etc.), incluyendo las fechas y horas relevantes. Además de archivar una versión electrónica, considere imprimir una copia.
- **Informar acerca del acoso por Internet a las autoridades apropiadas** – Si usted está siendo hostigado o amenazado, informe de esta actividad a las autoridades locales. Dependiendo de la actividad, también sería apropiado informar a los funcionarios del colegio que pueden tener políticas distintas para tratar con alguna actividad que involucre a los alumnos.

Proteja a sus hijos enseñándoles buenos hábitos cuando estén online. Mantengan líneas de comunicación abierta con sus hijos para que ellos se sientas cómodos contándole si fueron atacados online. Reduzca el riesgo de que sean acosados por Internet fijando pautas para navegar y monitoreando el uso que hacen de Internet y otros medios electrónicos (teléfonos celulares, Accesorios Personales Digitales (PDA), etc.).

2. Consejo de Seguridad Informática ST06-006

Saber qué son las Amenazas Ocultas: Archivos de Software Adulterados

El código malicioso no está siempre escondido en los *scripts* (guiones) de la página web o formatos de archivo no usuales. Los atacantes pueden adulterar o corromper tipos de archivos que usted reconocería y típicamente considera seguros, por lo tanto debe tener precaución cuando abra archivos provenientes de otras personas.

¿Qué tipos de archivos los atacantes pueden corromper o adulterar?

Un atacante puede insertar un código malicioso en cualquier archivo, incluyendo tipos de archivo comunes que usted normalmente consideraría seguros. Estos archivos pueden incluir documentos creados con un software de procesamiento de palabras, una planilla de cálculo, o archivos de imagen. Luego de corromper el archivo, un atacante puede distribuirlo a través del correo electrónico o publicarlo en un sitio web. Dependiendo del tipo de código malicioso, usted puede infectar su computadora sólo con abrir el archivo.

Cuando corrompen o adulteran archivos, los atacantes normalmente toman ventaja de las vulnerabilidades que descubren en el software que se usa para crear o abrir el archivo. Estas vulnerabilidades pueden permitir al atacante insertar y ejecutar scripts o código maliciosos, y no son siempre detectados. A veces la vulnerabilidad involucra una combinación de ciertos archivos (tales como un software en particular que está corriendo en un sistema operativo en particular) o solo afecta ciertas versiones de un programa de software.

¿Qué problemas pueden causar los archivos adulterados?

Hay varios tipos de código malicioso, incluyendo virus, gusanos y Troyanos. Sin embargo, el rango de consecuencias varía aún dentro de estas categorías. El código malicioso puede estar diseñado para realizar una o más funciones, incluyendo:

- Interferir con la habilidad de su computadora para procesar información consumiendo memoria o ancho de banda (provocando que su computadora se ponga significativamente lenta o aún “se cuelgue”)
- instalar, alterar, o eliminar archivos en su computadora
- brindar al atacante acceso a su computadora
- usar su computadora para atacar otras computadoras

¿Cómo puede protegerse?

- **Usar y mantener un software anti-virus** – El software anti-virus reconoce y protege su computadora contra los virus más conocidos, por lo tanto usted puede detectar y sacar el virus antes de que haga algún daño. Debido a que los atacantes están continuamente escribiendo nuevos virus, es importante mantener sus definiciones actualizadas.
- **Tener precaución con los adjuntos de correo electrónico** – No abra los adjuntos de correos electrónicos que usted no estaba esperando, especialmente si provienen de gente que no conoce. Si decide abrir un adjunto de correo electrónico, primero debe escanearlo para detectar si tiene virus. No sólo es posible que los atacantes "falsifiquen" (spoof) la fuente de un mensaje de correo electrónico, sino que sus contactos legítimos pueden enviarle a usted un archivo infectarlo sin saberlo.
- **Esté atento a los archivos que estén en la web para bajarlos** – Evite bajar archivos desde sitios que no confía. Si está obteniendo archivos de un sitio

supuestamente seguro, busque un certificado de sitio web. Si usted baja un archivo de un sitio web, considere guardarlo en su computadora y escanearlo manualmente para verificar si tiene virus antes de abrirlo.

- **Mantenga el software actualizado**- Instalar parches de software para que los atacantes no puedan tomar ventaja de problemas o vulnerabilidades conocidas. Muchos sistemas operativos ofrecen actualizaciones automáticas. Si esta opción está disponible, usted debería habilitarla.
- **Tome ventaja de los valores de seguridad** – Verifique los valores de seguridad de su cliente de correo electrónico y su navegador web. Aplique el más alto nivel de seguridad disponible que la funcionalidad que necesite.

Información Relacionada

- Securing Your Web Browser http://www.us-cert.gov/reading_room/securing_browser/ - Asegurar su Navegador Web
- Recovering from Viruses, Worms, and Trojan Horses http://www.us-cert.gov/cas/tips/ST05-006.html - Recuperarse de Virus, Gusanos y Caballos Troyanos.

3. Saber qué son las Amenazas Ocultas: Rootkits y Botnets

Los atacantes están permanentemente encontrando nuevas formas de acceder a los sistemas de computación. El uso de métodos ocultos tales como rootkits y botnets aumentó, y usted puede ser una víctima sin siquiera darse cuenta de ello.

¿Qué son los rootkits y botnets?

Un **rootkit** es un software que puede ser instalado y escondido en su computadora sin su conocimiento. Puede estar incluido en una paquete de software más grande o instalado por un atacante que pudo tomar ventaja de una vulnerabilidad en su computadora o lo ha convencido de que lo baje. Los rootkits no son necesariamente maliciosos, pero pueden esconder actividades maliciosas. Los atacantes pueden acceder a información, monitorear sus acciones, modificar programas, o realizar otras funciones en su computadora sin ser detectados.

Botnet es un vocablo que deriva de la idea de *bot networks* (redes bot - un **bot** - acortamiento de robot - es un programa informático que realiza funciones muy diversas, imitando el comportamiento de un humano). En su forma más básica, un bot es simplemente un programa de computadora automatizado, o robot. En el contexto de los *botnets*, bots se refiere a computadoras que pueden ser controladas por una, o muchas fuentes externas. Un atacante generalmente gana control infectando las computadoras con un virus u otro código malicioso que le da acceso al atacante. Su computadora puede ser parte de un botnet aunque parezca estar funcionando normalmente. Los botnets generalmente se usan para conducir un rango de

actividades, desde distribuir spam hasta virus para conducir ataques de denegación de servicio.

¿Por qué se los considera una amenaza?

El mayor problema con los rootkits tanto como con los botnets es que están escondidos. Aunque los botnets no están escondidos de la misma forma que están los rootkits, pueden no ser detectados a menos que usted esté específicamente buscando una cierta actividad. Si se ha instalado un rootkit, usted puede no darse cuenta que su computadora está comprometida, y el software anti-virus tradicional puede no detectar programas maliciosos. Los atacantes también están creando programas más sofisticados que se actualizan solos por lo que son aún más difíciles de detectar.

Los atacantes pueden usar rootkits y botnets para acceder y modificar información personal, atacar otra computadora, y cometer delitos, todo mientras permanecen sin ser detectados. Usando múltiples computadoras, los atacantes aumentan el rango e impacto de sus delitos. Debido a que cada computadora en un botnet puede estar programada para ejecutar el mismo comando, un atacante puede tener a cada uno escaneando múltiples computadoras para detectar vulnerabilidades, monitorear actividad online, o recolectar información ingresada en formularios online.

¿Qué puede hacer para protegerse?

Si usted tiene como rutina buenos hábitos de seguridad, puede reducir el riesgo de que su computadora pueda ser afectada:

- **Usar y mantener un software anti-virus –** El software anti-virus reconoce y protege su computadora contra los virus más conocidos, para que puede detectar y eliminar el virus antes de que pueda provocar un daño. Debido a que los atacantes están permanentemente escribiendo nuevos virus, es importante mantener las definiciones actualizadas. Algunos proveedores de anti-virus también ofrecen software anti-rootkit.
- **Instalar un firewall –** Los firewalls pueden prevenir algunos tipos de infecciones bloqueando el tráfico malicioso antes de que entre en su computadora y limitando el tráfico que usted envía. Algunos sistemas operativos realmente incluyen un firewall, pero debe asegurarse que esté habilitado.
- **Usar buenas contraseñas** - Seleccione contraseñas que serán difíciles de adivinar para los atacantes, y usar diferentes contraseñas para diferentes programas y dispositivos. No elija opciones que le permitan a su computadora recordar sus contraseñas.
- **Mantener el software actualizado**- Instalar parches de software para que los atacantes no puedan tomar ventaja de problemas o vulnerabilidades conocidos. Muchos sistemas operativos ofrecen actualizaciones automáticas. Si esta opción está disponible, usted debería habilitarla.
- **Seguir buenas prácticas de seguridad** - Tomar las precauciones adecuadas cuando use correo electrónico y navegadores web para reducir el riesgo de que sus acciones disparen una infección.

Lamentablemente, si hay un rootkit en su computadora o si un atacante está usando su computadora en un botnet, usted puede no saberlo. Aún si descubre que usted es una víctima, es difícil para el usuario promedio recuperar este episodio en forma efectiva. El atacante pudo haber modificado archivos en su computadora, por lo tanto simplemente eliminando los archivos maliciosos puede no resolver el problema, y no podrá confiar con seguridad de una versión previa de un archivo. Si usted cree que es una víctima, considere contactar a un administrador de sistema capacitado.

Como alternativa, algunos proveedores están desarrollando productos y herramientas que pueden sacar un rootkit de su computadora. Si el software no puede localizar y sacar la infección, usted puede necesitar reinstalar su sistema operativo, generalmente con un disco para restaurar el sistema que generalmente se provee con una nueva computadora. Tenga en cuenta que reinstalar o restaurar el sistema operativo generalmente borra todos sus archivos y cualquier software adicional que haya instalado en su computadora. También, la infección puede estar ubicada a un nivel tan profundo que no puede ser removida simplemente por medio de la reinstalación o restauración del sistema operativo.

4. Consejo de Seguridad Informática ST05-019

Prevenir y Responder a un Robo de Identidad

El robo de identidad, o fraude de identificación, es un delito que puede tener sustanciales consecuencias financieras y emocionales. Tener precaución con la información personal, y su usted se tornó en una víctima, actúe inmediatamente para minimizar el daño.

¿El robo de identidad es solo un problema para gente que pone información online?

Usted puede ser una víctima de robo de identidad aún si nunca usó una computadora. La gente maliciosa puede obtener información personal (tal como números de tarjeta de crédito, números de teléfono, números de cuenta, y direcciones) al robarle su billetera o cartera, escuchando una conversación telefónica, revolviendo su basura (una práctica conocida como buceando en los contenedores), o tomando un ticket de un restaurant que tenga su número de cuenta en él. Si un ladrón tiene suficiente información, puede hacerse pasar por usted para comprar objetos, abrir nuevas cuentas, o solicitar préstamos.

Internet ha facilitado a los ladrones la obtención de información personal y financiera. La mayoría de las empresas y otras instituciones guarda la información sobre sus clientes en bases de datos; si un ladrón puede acceder a esa base de datos, puede obtener información acerca de muchas persona de una sola vez en lugar de ir de a una por vez. Internet también facilitó a los ladrones vender o comercializar información,

haciendo que a los que deben aplicar la ley les resulte más difícil identificar y aprehender a los delincuentes.

¿Cómo se elige a las víctimas de robo de identidad online?

El robo de identidad generalmente es un delito de oportunidad, por lo tanto usted puede ser una víctima debido a que su información está disponible. Los ladrones pueden apuntar a los clientes de ciertas empresas por una variedad de motivos; por ejemplo, una base de datos de una empresa es fácilmente accesible, la demografía de los clientes es atractiva, o hay un mercado para información específica. Si su información está almacenada en una base de datos que está comprometida, usted se puede tornar en una víctima de robo de identidad.

¿Hay formas de evitar ser una víctima?

Lamentablemente, no hay forma de garantizar que usted no será una víctima de robo de identidad online. Sin embargo, hay formas de minimizar su riesgo:

- **Hacer negocios con empresas de reputación** – Antes de dar cualquier información personal o financiera, asegúrese que usted está interactuando con una empresa de reputación y establecida. Algunos atacantes pueden tratar de engañarlo creando sitios web maliciosos que parecen ser legítimos, por lo tanto debería verificar la legitimidad antes de proveer cualquier.
- **Tomar ventaja de las características/opciones de seguridad** – Las contraseñas y otras características/opciones de seguridad agregan capas de protección si se las utiliza en forma adecuada.
- **Verificar las políticas de seguridad** – Tome precauciones cuando suministre información, y asegúrese de verificar las políticas de privacidad publicadas para ver cómo la empresa usará o distribuirá su información. Muchas empresas permiten a sus clientes solicitar que su información no sea compartida con otras empresas; podría ubicar los detalles de información de su cuenta o contactar directamente a la empresa.
- **Tener cuidado con la información que publicite** – Los atacantes pueden armar toda su información a partir de una variedad de fuentes. Evite publicar datos personales en foros públicos.
- **Usar y mantener software anti-virus y un firewall** – Protéjase de los virus y Troyanos que puedan robarle o modificar los datos en su propia computadora y dejarlo vulnerable usando un software anti-virus y un firewall. Asegúrese de mantener sus definiciones de virus actualizadas.
- **Estar atento a la actividad de su cuenta** – Preste atención a sus resúmenes de cuentas y verifique el informe de tarjeta de crédito anualmente.

¿Cómo saber si su identidad fue robada?

Las empresas tienen distintas políticas para notificar a los clientes cuando descubren que alguien tuvo acceso a la base de datos de clientes. Sin embargo, usted debería

atento a los cambios en la actividad normal de su cuenta. Los siguientes son ejemplos de cambios que indicarían que alguien tuvo acceso a su información:

- Cargos no usuales o inexplicables en sus cuentas
- Llamadas telefónicas o facturas por cuentas, productos o servicios que usted no tiene
- Dejar de recibir facturas o correos corrientes
- Cuentas nuevas y extrañas que aparecen en su resumen de tarjeta de crédito
- Rechazo inesperado de su tarjeta de crédito

¿Qué puede hacer si piensa o sabe que han robado su identidad?

Recuperarse de un robo de identidad puede ser un proceso largo, estresante y potencialmente costoso. Muchas empresas de tarjeta de crédito han adoptado políticas para tratar de minimizar el monto de dinero por el cual usted es responsable, pero las consecuencias pueden extenderse más allá de sus cuentas existentes. Para minimizar el grado del daño, tome acciones lo antes posible:

- **Contacte a las empresas, incluyendo bancos, donde usted tiene cuentas** – Informe a las empresas donde usted tiene cuentas que alguien puede estar usando su identidad, e investigue su hubieron transacciones no autorizadas. Cierre cuentas para que los cargos futuros sean rechazados. Además de llamar a la empresa, mande una carta para que quede registro del problema.
- **Contacte a las principales empresas de información sobre crédito** – Verifique su informe de crédito para ver si hubo alguna actividad no esperada o no autorizada. Ponga una alerta de fraude en los informes de su crédito para prevenir que se abran nuevas cuentas sin verificación.
- **Considere otra información que pueda estar en riesgo** – Dependiendo de qué información fue hurtada, puede necesitar contactar otras instituciones; por ejemplo, si un ladrón tuvo acceso a su número de Seguridad Social, contáctese con la ANSES o la AFIP según corresponda. También debería contactar al Registro del Automotor si le robaron su registro de conducir o el título de propiedad de su automóvil.

5. Consejo de Seguridad Informática ST05-006

Recuperación de Virus, Gusanos y Troyanos

Lamentablemente, muchos usuarios son víctimas de virus, gusanos o Troyanos. Si su computadora se infectara con un código malicioso, hay pasos que debe tomar para superarlo.

¿Cómo sabe que su computadora está infectada?

Lamentablemente, no hay una forma particular para identificar que su computadora fue infectada con un código malicioso. Algunas infecciones pueden destruir completamente archivos y apagar su computadora, mientras que otras pueden afectar las operaciones normales de su computadora en forma más tenue. Esté atento a cualquier conducta inusual o inesperada. Si está corriendo un software anti-virus, éste lo puede alertar que encontró un código malicioso en su computadora. El software anti-virus puede limpiar el código malicioso automáticamente, pero si no puede, necesitará tomar pasos adicionales.

¿Qué puede hacer si su computadora está infectada?

1. **Minimizar el daño** – Si está en el trabajo y tiene acceso al departamento de Tecnología de la Información, contáctelos inmediatamente. Lo antes que puedan investigar y limpiar su computadora, menor será el daño a ella y otras computadoras de la red. Si está en la computadora o laptop de su casa, desconéctela de Internet. Sacando la conexión a Internet, previene que un atacante o un virus pueda acceder a su computadora y realizar tareas tales como ubicar datos personales, manipular o eliminar archivos, o usar su computadora para atacar otras computadoras.
2. **Eliminar el código malicioso** – Si tiene instalado un software anti-virus en su computadora, actualice las definiciones de virus (si fuere posible), y realice un escaneo manual de todo el sistema. Si no tiene un software anti-virus, puede comprarlo en el negocio de ventas de estos productos para computadoras. Si el software no puede localizar y eliminar la infección, puede necesitar reinstalar su sistema operativo, generalmente con un disco de restauración del sistema que generalmente viene provisto con computadoras nuevas. Tenga en cuenta que reinstalar y restaurar el sistema operativo típicamente borra todos los archivos y cualquier software adicional que haya instalado en su computadora. Luego de reinstalar el sistema operativo y cualquier otro software, instale todos los parches adecuados para enmendar las vulnerabilidades conocidas.

¿Cómo puede reducir el riesgo de otra infección?

Tratar con un código malicioso en su computadora puede ser una experiencia frustrante que puede costar tiempo, dinero y datos. Las siguientes recomendaciones construirán su defensa contra futuras infecciones:

- **Usar y mantener un software anti-virus** – El software anti-virus reconoce y protege su computadora contra la mayoría de los virus conocidos. Sin embargo, los atacantes están permanentemente liberando nuevos virus, por lo tanto es importante que mantenga su software anti-virus actualizado.
- **Cambiar sus contraseñas** – Sus contraseñas originales pudieron quedar comprometidas durante la infección, por lo tanto cámbielas. Esto incluye las contraseñas para sitios web que pudieron haber quedado en “caché” en su navegador. Haga contraseñas que sean difíciles de adivinar por los atacantes.

- **Mantener el software actualizado** – Instalar parches al software para que los atacantes no tomen ventaja de problemas o vulnerabilidades conocidas. Muchos sistemas operativos ofrecen actualizaciones automáticas. Si esta opción está disponible, debería habilitarla.
- **Instalar o habilitar un firewall** – Los firewalls puede prevenir algunos tipos de infección bloqueando el tráfico malicioso antes de que ingrese a su computadora. Algunos sistemas operativos en realidad incluyen un firewall, pero debe asegurarse que esté habilitado.
- **Usar herramientas anti-spyware** - Spyware es una fuente común de virus, pero usted puede minimizar la cantidad de infecciones usando un programa legítimo que identifica y elimine el spyware.
- **Seguir buenas prácticas de seguridad** - Tome las precauciones adecuadas cuando use el correo electrónico y los navegadores web para poder reducir el riesgo de que sus acciones disparen una infección.

Como precaución, mantenga backups de sus archivos en CDs o DVDs para tener copias guardadas en caso de volver a quedar infectado.

Información adicional

- Recuperación de un Caballo Troyano o Virus - http://www.us-cert.gov/reading_room/trojan-recovery.pdf
- Antes de Conectar una Nueva Computadora a Internet - http://www.us-cert.gov/reading_room/before_you_plug_in.html
- Asegurar su Navegador Web - http://www.us-cert.gov/reading_room/securing_browser/

6. Consejo de Seguridad Informática ST04-016

Reconocer y Evitar Spyware

Debido a su popularidad, Internet se convirtió en un blanco para la publicidad. Como resultado de esto, spyware o adware, son cada vez más corrientes. Cuando esté buscando detectar un problema con su computadora, puede descubrir que la fuente del problema es un software spyware que fue instalado en su máquina sin su conocimiento.

¿Qué es un spyware?

A pesar de su nombre, el término "spyware" *(“spy” significa “espía”)* no se refiere a algo utilizado por operadores secretos, sino por la industria de la publicidad. En realidad, spyware también es conocido como "adware". Se refiere a una categoría de software que, cuando está instalado en su computadora, puede enviar propagandas como ventanas emergentes, redireccionar su buscador a ciertos sitios web, o monitorear los sitios web que usted visita. Algunas versiones de spyware invasivas y

extremas pueden rastrear con exactitud qué teclas tipea. Los atacantes también pueden usar spyware para fines maliciosos.

Debido a un procesamiento extra, spyware puede hacer que su computadora se torne lenta o perezosa. También hay consecuencias en cuanto a la privacidad:

- ¿Qué información se está reuniendo?
- ¿Quién la está recibiendo?
- ¿Cómo está siendo utilizada?

¿Como saber si hay spyware en su computadora?

Los siguientes síntomas *pueden* indicar que hay spyware instalado en su computadora:

- Usted está sometido a interminables ventanas emergentes
- Usted es redireccionado a sitios web que no son los que tipeó en su navegador
- En su navegador web aparecen barras de herramientas nuevas e inesperadas
- En la bandeja de entrada en la parte inferior de su pantalla aparecen íconos no esperados
- La página principal de su navegador cambió abruptamente
- El buscador que su navegador abre cuando usted cliquea “buscar” ha cambiado
- Algunas teclas dejan de funcionar en su navegador (por ejemplo, la tecla de tabulación no funciona cuando está pasando al siguiente campo en un formulario)
- Empiezan a aparecer errores de mensajes Windows en forma aleatoria
- Su computadora repentinamente se pone muy lenta cuando abre programas o realiza tareas (guardar archivos, etc.)

¿Cómo puede prevenir que se instale un spyware en su computadora?

Para evitar instalarlo usted mismo en forma no intencional, siga estas buenas prácticas de seguridad:

- **No cliquear links con ventanas emergentes** – Como las ventanas emergentes generalmente son un producto del spyware, al cliquear sobre una ventana se puede instalar el software spyware en su computadora. Para cerrar la ventana emergente, cliquear el ícono "X" en la barra del título en lugar del link "cerrar " *(close*) dentro de la ventana.
- **Contestar "no" cuando reciba preguntas inesperadas** – Esté atento a las ventanas de diálogo inesperados preguntando si usted quiere correr un programa en particular o realizar algún otro tipo de tarea. Siempre seleccione "no" o "cancelar," o cierre la ventana de diálogo cliqueando en el ícono "X" en barra del título.
- **Estar atento al software que se baja gratis** – Hay muchos sitios que ofrecen barras de herramientas personalizadas u otras características que pueden resultar atractivas a los usuarios. No bajar programas de sitios de los que no confía y tome conciencia de que puede estar exponiendo su computadora a un spyware bajando algunos de estos programas.

- **No seguir links de correo electrónico que dicen ofrecer software anti-spyware** – Tal como los virus de correo electrónico, los links pueden tener el fin opuesto y en realidad instalar el spyware que dicen eliminar.

Como una buena práctica de seguridad adicional, especialmente si usted está preocupado por si tuviera un spyware en su máquina y quiere minimizar el impacto, considere tomar la siguiente acción:

- **Ajuste las preferencias de su navegador para limitar las ventanas emergentes y las cookies** – Las ventanas emergentes generalmente están generadas por algún tipo de script o contenido activo. Ajustando los valores/configuración dentro de su navegador para reducir o prevenir algún tipo de script o contenido activo puede reducir la cantidad de ventanas emergentes que aparecen. Algunos navegadores ofrecen una opción específica para bloquear o limitar las ventanas emergentes. Algunos tipos de cookies a veces son consideradas spyware porque revelan qué páginas web usted visitó. Puede ajustar sus valores/configuración de privacidad para permitir cookies sólo para el sitio web que está visitando.

¿Como eliminar los spyware?

- **Haga correr un escaneo completo en su computadora y su software anti-virus** – Algunos software anti-virus encontrarán y eliminarán spyware, pero puede no encontrar el spyware cuando esté monitoreando su computadora en tiempo real. Configurar su software anti-virus para que le solicite correr un escaneo completo periódicamente.
- **Corra un producto legítimo específicamente diseñado para eliminar spyware** – Muchos proveedores ofrecen productos que escanearán su computadora para detectar spyware y eliminar cualquier software spyware. Los productos populares incluyen el Ad-Aware de Lavasoft, el Window Defender de Microsoft, el SpySweeper de Webroot, y el Spybot Search and Destroy.
- **Asegúrese que su software anti-virus y anti-spyware son compatibles** – Haga una instalación del software por fase para asegurarse que no está provocando problemas no intencionales.

7. Consejo de Seguridad Informática ST04-014

Evitar Ataques de Ingeniería Social y Phising

No proporcione información delicada a nadie a menos que usted esté seguro que ellos son realmente los que dicen ser y que deberían tener acceso a la información.

¿Qué es un ataque de ingeniería social?

En un ataque de ingeniería social, un atacante usa interacción humana (habilidades sociales) para obtener o comprometer información acerca de una organización o sus sistemas de computación. Un atacante puede parecer sin pretensiones y respetable, posiblemente pretendiendo ser un nuevo empleado, una persona de reparación, o un investigador, y aún ofrecer credenciales para sustentar su identidad. Sin embargo, haciendo preguntas, el atacante puede armar y reunir información suficiente para infiltrarse en la red de una organización. Si un atacante no puede reunir información suficiente de una fuente, puede contactar otra fuente dentro de la misma organización o confiar en la información de la primera fuente para agregar su credibilidad.

¿Qué es un ataque phishing?

Phishing es una forma de ingeniería social. Los ataques phishing usan el correo electrónico o sitios web maliciosos para solicitar información personal presentándose como una organización confiable. Por ejemplo, un atacante puede enviar un correo electrónico desde una empresa acreditada de tarjetas de crédito o institución financiera que requiere información sobre la cuenta, generalmente sugiriendo que hay un problema. Cuando los usuarios responden con la información solicitada, los atacantes pueden usarla para ganar acceso a las cuentas.

Los ataques phishing también pueden parecer provenir de otros tipos de organización, tales como organizaciones de caridad. Los atacantes generalmente sacan ventaja de eventos presentes y ciertas épocas del año, tales como:

- Desastres naturales (por ejemplo, Huracán Katrina, tsunami en Indonesia)
- Epidemias y amenazas a la salud (por ejemplo, H1N1)
- Preocupaciones económicas (por ejemplo estafas de la Agencia de Recaudación)
- Elecciones políticas principales
- Feriados

¿Cómo evitar ser una víctima?

- Sospeche de llamadas telefónicas, visitas o mensajes de correo electrónico no solicitados, provenientes de individuos que le preguntan acerca de empleados u otra información interna. Si un individuo desconocido dice provenir de una organización legítima, trate de verificar su identidad directamente en la empresa.
- No suministre información personal o información acerca de su organización, incluyendo su estructura o redes, a menos que esté seguro de la autoridad que tiene esa persona para tener la información.
- No revele información personal o financiera en el correo electrónico, y no responda a correos electrónicos solicitando esta información. Esto incluye seguir links enviados en un correo electrónico.

- No envíe información delicada o privada por Internet antes de verificar la seguridad del sitio web.
- Preste atención al URL de un sitio web. Los sitios web maliciosos pueden tener el mismo aspecto que uno legítimo, pero el URL puede usar una variación en la ortografía o un dominio diferente (por ejemplo, .com vs. .net).
- Si no está seguro que la solicitud de un correo electrónico es legítima, trate de verificarlo contactando a la empresa directamente. No use información de contacto suministrada en un sitio web conectado con la solicitud; en cambio, verifique las declaraciones o comunicados previos para información de contacto. También hay información disponible online acerca de ataques phishing conocidos proveniente de grupos tales como el Grupo de Trabajo Anti-Phishing (Anti-Phishing Working Group) (http://www.antiphishing.org).
- Instale y mantenga un software anti-virus, firewalls, y filtros de correo electrónico para reducir parte de este tráfico.
- Tome ventaja de cualquier característica anti-phishing ofrecida por su cliente de correo electrónico y navegador web.

¿Qué hacer si piensa que es una víctima?

- Si cree que podría haber revelado información delicada y probada acerca de su organización, infórmelo a la gente apropiada dentro de la organización, incluyendo los administradores de la red. Ellos pueden estar alertas a cualquier actividad sospechosa o inusual.
- Si cree que sus cuentas financieras pueden estar comprometidas, contacte a la institución financiera inmediatamente y cierre cualquier cuenta que pudiera haber sido comprometida. Verifique si hay algún cargo inexplicable en su cuenta.
- Inmediatamente cambie cualquiera de las contraseñas que pudiera haber revelado. Si usó la misma contraseña para recursos múltiples, asegúrese de cambiarla para cada cuenta, y no use esa contraseña en el futuro.
- Verifique si hay otros signos de robo de identidad.

8. Consejo de Seguridad Informática ST04-015

Saber qué es un Ataque de Denegación de Servicio - *(DoS)*

Usted habrá escuchado acerca de los ataques de denegación de servicio lanzados contra sitios web, pero usted también puede ser una víctima de estos ataques. Los ataques de denegación de servicio pueden ser difíciles de distinguir de una actividad de red común, pero hay algunas indicaciones de que el ataque está en progreso.

¿Qué es un ataque de denegación de servicio?

En un ataque de denegación de servicio (*denial-of-service - DoS*), un atacante intenta que los usuarios legítimos no puedan acceder a la información o servicios. Tomando

como objetivo su computadora y su conexión de red, o las computadoras y red de los sitios que usted está tratando de usar, un atacante puede prevenir que usted acceda al correo electrónico, sitios web, cuentas online (operaciones bancarias, etc.), u otros servicios que se soportan sobre la computadora afectada.

El tipo de ataque de denegación de servicio más común obvio ocurre cuando un atacante "inunda" una red con información. Cuando usted tipea un URL para un sitio web en particular dentro de su navegador, usted está enviando un pedido al servidor de la computadora de ese sitio para ver la página. El servidor sólo puede procesar una cierta cantidad de pedidos a la vez, por lo tanto si un atacante sobrecarga el servidor con pedidos, éste no puede procesar el suyo. Esto es un "ataque de denegación de servicio" porque usted no puede acceder al sitio.

Un atacante puede usar mensajes de correo electrónico spam para lanzar un ataque similar sobre su cuenta de correo electrónico. Si usted tiene una cuenta de correo electrónico provista por su empleador o disponible a través de un servicio gratis como Yahoo o Hotmail, usted tiene asignado un cupo específico que limita la cantidad de datos que puede tener en su cuenta en un momento dado. Enviando mensajes de correo electrónico en gran cantidad o muy largos a la cuenta, un atacante puede consumir su cupo, previniendo que pueda recibir mensajes legítimos.

¿Qué es un ataque de denegación de servicio distribuido – (*DdoS)*?

En un ataque de denegación de servicio distribuido (*distributed denial-of-service - DDoS*), un atacante puede usar su computadora para atacar a otra computadora. Tomando ventaja de las vulnerabilidades o debilidades de seguridad, un atacante podría tomar control de su computadora. Éste podría entonces forzar a su computadora a reenviar una gran cantidad de datos a un sitio web o enviar spam a una dirección de correo electrónico en particular. El ataque es "distribuido" porque el atacante está usando computadoras múltiples, incluyendo la suya, para lanzar un ataque de denegación de servicio.

¿Cómo evitar ser parte del problema?

Lamentablemente, no hay formas efectivas de prevenir un ataque de denegación de servicio o un ataque de denegación de servicio distribuido, pero hay pasos que puede tomar para reducir la probabilidad de que un atacante use su computadora para atacar otras computadoras:

- Instalar y mantener un software anti-virus.
- Instalar un firewall, y configurarlo para que restrinja el tráfico entrante y saliente de su computadora.
- Seguir buenas prácticas de seguridad para la distribución de las direcciones de su correo electrónico. Aplicando filtros de correo electrónico puede ayudar a manejar el tráfico no deseado.

¿Cómo saber si está ocurriendo un ataque?

No todas las interrupciones del servicio son el resultado de un ataque de denegación de servicio. Puede haber muchos problemas técnicos con una red en particular, o los

administradores del sistema pueden estar haciendo mantenimiento. Sin embargo, los siguientes síntomas *podrían* indicar un ataque DoS o DDoS:

- Un funcionamiento de la red inusualmente lento (al abrir archivos o acceder a sitios web)
- No disponibilidad de un sitio web en particular
- Imposibilidad de acceder a algún sitio web
- Aumento alarmante en la cantidad de spam que recibe en su cuenta

¿Qué hacer si piensa que está experimentando un ataque?

Aún si puede identificar correctamente un ataque DoS o DDoS, será poco probable que usted puede determinar el objetivo real o fuente del ataque. Solicitar asistencia a los profesionales adecuados.

- Si observa que no puede acceder a sus propios archivos o alcanzar cualquier sitio web externo desde su computadora, contactar a sus administradores de la red. Esto puede indicar que su computadora o la red de su organización está siendo atacada.
- Si está teniendo una experiencia similar en la computadora de su casa, considere contactar a su proveedor de servicio de Internet (PSI). Si hay un problema, el PSI podría aconsejarle una acción apropiada a seguir.

9. Consejo de Seguridad Informática ST04-009

Identificar Engaños (*Hoaxes*) y Leyendas Urbanas

Las cartas en cadena son familiares para cualquier persona con una cuenta de correo electrónico, ya fuere los enviados por extraños o de amigos o miembros de la familia bien intencionados. Trate de verificar la información antes de seguir cualquier instrucción o seguir pasando el mensaje.

¿Por que las cartas en cadena son un problema?

El problema más serio es que las cartas en cadena pueden enmascarar virus u otra actividad maliciosa. Pero aún las que parecen ser inofensivas pueden tener repercusiones negativas si usted las pasa:

- Consumen banda ancha o espacio dentro de la casilla de mensajes entrantes del receptor.
- Fuerza a la gente que conoce a perder tiempo filtrando los mensajes y posiblemente utilizando tiempo para verificar la información.
- Está desparramando información exagerada y, a menudo, temor o paranoia innecesarios.

¿Cuáles son algunos tipos de cartas en cadena?

Hay dos tipos principales de cartas en cadena:

- **Engaños (*Hoaxes*)** – Los engaños intentan burlar o defraudar a los usuarios. Un engaño podría ser malicioso, solicitando a los usuarios que borren un archivo necesario para el sistema operativo indicando que eso es un virus. También podría ser una estafa que convence a los usuarios para que envíen dinero o información personal. Los ataques Phishing podrían caer en esta categoría.
- **Leyendas Urbanas** – Las leyendas urbanas están diseñadas para ser redistribuidas y generalmente alertan a los usuarios de una amenaza o dicen estar notificándolos de una información importante o urgente. Otra forma común son los correos electrónicos que prometen a los usuarios recompensas de dinero por direccionar el mensaje o sugerir que están firmando algo que será presentado a un grupo en particular. Las leyendas urbanas generalmente no tienen efecto negativo más que pérdida de ancho de banda y tiempo.

¿Cómo puede establecer si el correo electrónico es un engaño (hoax) o una leyenda urbana?

Algunos mensajes son más sospechosos que otros, pero especialmente hay que tener cuidado si el mensaje tiene cualquiera de las características enumeradas debajo. Estas características son sólo una guía – no todo *hoax* o leyenda urbana tiene estos atributos-, y algunos mensajes legítimos pueden tener algunas de estas características:

- Sugiere que hay consecuencias trágicas por no realizar la acción
- Promete dinero o certificados de regalos por realizar la acción
- Ofrece instrucciones o adjuntos que pretenden protegerlo de un virus que no es detectado por el software anti-virus
- Pretende no ser un *hoax*
- Hay múltiples errores de ortografía o gramática, o la lógica es contradictoria
- Hay una aseveración que lo apura a que distribuya el mensaje
- Ya ha sido distribuido múltiples veces (evidente desde los encabezamientos del correo electrónico en el cuerpo del mensaje)

Si quiere confirmar la validez de un correo electrónico, hay algunos sitios web que dan información acerca de *hoaxes* y leyendas urbanas:

- Leyendas Urbanas y Flolklore - http://urbanlegends.about.com/
- Páginas de Referencia de Leyendas Urbanas - http://www.snopes.com/
- TruthOrFiction.com - http://www.truthorfiction.com/
- Symantec Security Response Hoaxes - http://www.symantec.com/avcenter/hoax.html
- McAfee Security Virus Hoaxes - http://vil.mcafee.com/hoax.asp

10. Consejo de Seguridad Informática ST06-004

Evitar las Trampas en Transacciones Comerciales Online

Las transacciones comerciales online pueden ser fáciles, y una forma efectiva desde el punto de vista de costos para manejar inversiones. Sin embargo, los inversores online a menudo son objetivos para estafas, por lo tanto tome precauciones para asegurarse que no se tornará en una víctima.

¿Qué es una transacción comercial online?

Las transacciones comerciales online le permiten llevar a cabo transacciones de inversión por Internet. La accesibilidad de Internet hace posible que usted pueda investigar e invertir en oportunidades desde cualquier lugar y a cualquier hora. También reduce la cantidad de recursos (tiempo, esfuerzo y dinero) que necesita dedicarle para manejar estas cuentas y transacciones.

¿Cuáles son los riesgos?

Reconocer la importancia de salvaguardar su dinero, los operadores/corredores de bolsa online legítimos toman pasos para asegurarse que sus transacciones son seguras. Sin embargo, los operadores y los inversores que los usan son objetivos atractivos para los atacantes. La cantidad de información financiera en la base de datos de los operadores la hace valiosa; esta información puede ser rastreada y vendida para provecho personal. También, porque el dinero es normalmente transferido a través de estas cuentas, la actividad maliciosa puede no ser notada inmediatamente. Para ganar acceso a estas bases de datos, los atacantes pueden usar Troyanos u otros tipos de código malicioso.

Los atacantes también pueden intentar reunir información financiera apuntando directamente a inversores actuales o potenciales. Estos intentos pueden tomar la forma de ataques de ingeniería social o ataques phishing. Con métodos que incluyen armar oportunidades de inversión fraudulentas o redireccionando a los usuarios a sitios maliciosos que parecen ser legítimos, los atacantes tratan de convencerlo para que les provea de información financiera que ellos pueden usar o vender. Si usted ya es una víctima, tanto su dinero como su identidad pueden estar en riesgo.

¿Cómo puede protegerse?

- **Investigar/buscar acerca de sus oportunidades de inversión** – Tomar ventaja de los recursos tales como la base de datos EDGAR de la Comisión de Valores y Bolsa de Los Estados Unidos (U.S. Securities and Exchange Comisión) y la Comisión de Bolsa de su PaísEstado para investigar a las empresas.
- **Estar atento a la información online** – Cualquier persona puede publicar información en Internet, por lo tanto trate de verificar cualquier investigación/búsqueda online a través de otros métodos antes de invertir

dinero. También tenga cuidado de las oportunidades de inversión "calientes" publicadas online o en el correo electrónico.

- **Verificar las políticas de privacidad** – Antes de suministrar información personal o financiera, verifique la política de seguridad del sitio web. Asegúrese que comprende cómo su información será almacenada y utilizada.
- **Asegurarse de que sus transacciones estén encriptadas** – Cuando la información se envía por Internet, los atacantes pueden interceptarla- El encriptado previene que los atacantes puedan ver la información.
- **Verificar que el sitio web sea legítimo** – Los atacantes pueden redireccionarlo a un sitio web malicioso que tiene un aspecto idéntico a uno legítimo. Pueden convencerlo para que les proporcione su información personal y financiera, que usan para su propio beneficio. Verificar el certificado del sitio web para asegurarse que es legítimo.
- **Monitorear sus inversiones** – Verifique con regularidad sus cuentas para detectar si hay alguna actividad inusual. Informe las transacciones no autorizadas en forma inmediata.
- **Usar y mantener un software anti-virus** – El software anti-virus reconoce y protege a su computadora contra los virus más conocidos. Sin embargo, como los atacantes están permanentemente liberando nuevos virus, es importante mantener sus definiciones de virus actualizadas.
- **Usar herramientas anti-spyware** - Spyware es una fuente de virus común, y los atacantes pueden usarlo para acceder a información en su computadora. Puede minimizar la cantidad de infecciones usando un programa legítimo que identifique y elimine spyware.
- **Mantener el software actualizado** – Instalar los parches del software para que los atacantes no puedan tomar ventaja de problemas o vulnerabilidades conocidos. Habilitar las actualizaciones automáticas si esta opción está disponible.

- **Evaluar sus valores/configuración de seguridad** – Ajustando los valores de seguridad en su navegador, puede limitar el riesgo de ciertos ataques.