Seguridad General

1. Consejo de Seguridad Informática ST04-002

Selección y Protección de Contraseñas (password)

Las contraseñas son una forma común de autenticación y generalmente son la única barrera entre el usuario y su información personal. Hay varios programas que los atacantes pueden usar para ayudar a adivinar o "craquear" contraseñas, pero eligiendo buenas contraseñas y manteniéndolas confidenciales, usted puede hacer más difícil que una persona no autorizada pueda acceder a su información.

¿Por qué usted necesita una contraseña?

Piense acerca de la cantidad de números de identificación personal (PINs), contraseñas, o frases claves que usted usa todos los días: para extraer dinero del cajero automático o usar su tarjeta de débito en un negocio, iniciar su sesión en la computadora o correo electrónico, registrarse e iniciar sesión en una cuenta de banco online (por Internet) o comprar por Internet con el carrito de compras ... la lista parece ser cada vez más larga. A veces puede ser frustrante mantener el control de todos los números, letras, y combinaciones de palabras, y quizás usted ha pensado si todo este lío vale la pena. Después de todo, ¿qué les interesa a los atacantes acerca de su cuenta de correo electrónico personal? o ¿por qué a alguien le interesaría su cuenta bancaria prácticamente vacía cuando hay otras con mucho más dinero? Generalmente, un ataque no es específicamente con referencia a su cuenta sino poder usar el acceso a su información para lanzar un ataque mayor. Y mientras que ganar algún acceso a su correo electrónico personal pudiera no parecer mucho más que un inconveniente o amenaza a su privacidad, piense en las consecuencias de un atacante que gana acceso a su número de seguridad social o sus registros médicos.

Una de las mejores formas de proteger la información y la propiedad física es asegurarse que sólo las personas autorizadas tengan acceso a ello. El siguiente paso es verificar que alguien es la persona que pretende ser, y este proceso de autenticación es aún más importante, y más difícil, en el mundo de la cibernética. Las contraseñas son los medios más comunes de autenticación, pero si usted no elije buenas contraseñas o no las mantiene en forma confidencial, son casi tan ineficientes como no tener ninguna contraseña. Muchos sistemas y servicios fueron invadidos exitosamente debido al uso de contraseñas inseguras o inadecuadas, y algunos virus y gusanos se introdujeron al sistema adivinando contraseñas débiles.

¿Cómo seleccionar una buena contraseña?

La mayoría de las personas usan contraseñas que están basadas en información personal y son fáciles de recordar. Esto también facilita a un atacante adivinarlas o "craquearles". Considere un número de identificación (PIN) de cuatro dígitos. ¿El suyo

es una combinación del mes, día o año de su cumpleaños? ¿O los cuatro últimos dígitos de su número de seguridad social? ¿O su domicilio o número de teléfono? Piense lo fácil que será encontrar esta información acerca de alguien. ¿Y qué sucede con su contraseña de correo electrónico – es una palabra que puede ser encontrada en el diccionario? Si fuere así, ésta puede ser susceptible a ataques de "diccionario", que intentan adivinar contraseñas basadas en palabras que están en el diccionario.

Aunque escribir mal una palabra intencionalmente ("daytt" en lugar de "date") puede ofrecer alguna protección contra los ataques de diccionarios, un buen método es confiar en una serie de palabras y usar técnicas de memoria o reglas mnemotécnicas, para ayudarlo a cómo decodificarlo. Use un acrónimo de algo fácil de recordar Ej: NorCarTren (Norma, Carlos, Tren). Añada un número al acrónimo para mayor seguridad Ej: NorCarTren09 (Norma, Carlos, Tren, Edad del hijo). Mejor aún, si la frase origen no es conocida por otros Ej: Verdel4ydos (Verano del 42). Elija una palabra sin sentido, aunque pronunciable. Ej: galpo-glio. Realice reemplazos de letras por signos o números. Ej: 3duard0palmit0. Elija una clave que no pueda olvidar, para evitar escribirla en alguna parte. Ej: arGentina6-0. Usar minúsculas y mayúscula le agrega un manto de oscuridad. **Su mejor defensa, sin embargo, es usar una combinación de números, caracteres especiales, y letras minúsculas y mayúsculas.**

Las contraseñas más largas son más seguras que las cortas porque hay más caracteres para adivinar. Por lo tanto, considere usar frases de contraseña cuando pueda. Usted tal vez tenga que probar diferentes variaciones de una frase contraseña – muchas aplicaciones limitan la extensión de las contraseñas, y algunas pueden no aceptar espacios. Evite frases comunes, citas comunes y letras de canciones.

No asuma que ahora que usted desarrolló una contraseña fuerte debería usarla para todos los sistemas o programas en los que se registra. Si un atacante adivina esto, podría tener acceso a todas sus cuentas. Usted debería usar estas técnicas para desarrollar contraseñas únicas para cada una de sus cuentas.

Aquí se muestra una revisión de las tácticas a usar cuando se elija una contraseña:

- No utilice contraseñas que estén basadas en información personal a la que se puede acceder o adivinar fácilmente.
- No use palabras que puedan encontrarse en cualquier diccionario de cualquier idioma.
- Desarrolle una regla mnemotécnica para recordar contraseñas complejas.
- Use letras mayúsculas y minúsculas.
- Use una combinación de letras, números y caracteres especiales.
- Use frases contraseña cuando pueda.
- Use contraseñas diferentes en sistemas diferentes.

¿Cómo puede proteger su contraseña?

Ahora que ha elegido una contraseña que es difícil de adivinar, se tiene que asegurar de no dejarla en algún lugar que la gente la pueda encontrar. Anotarla y dejarla sobre

su escritorio, cerca de su computadora, o peor, pegarla con cinta en su computadora, es sólo facilitársela a alguien que tenga acceso físico a su oficina. No le diga a nadie sus contraseñas, y esté atento a atacantes que traten de engañarlo a través de llamadas telefónicas o mensajes de correo electrónico solicitándole que revele sus contraseñas.

Si su proveedor de servicio de Internet (PSI) ofrece elecciones de sistemas de autenticación, busque aquellos que usan Kerberos (un protocolo de autenticación de redes de computadoras que permite a dos computadores en una red insegura demostrar su identidad mutuamente de manera segura), método de autenticación desafío/respuesta, o encriptado de clave pública, más que simples contraseñas. Considere a los proveedores de servicio exigentes que sólo usan contraseñas para adoptar métodos más seguros.

También muchos programas ofrecen la opción de "recordar" su contraseña, pero estos programas tienen distintos grados de seguridad que protegen esa información. Dichos programas, tales como clientes de correo electrónico, almacenan la información en un texto claro en un archivo en su computadora. Esto significa que cualquier persona con acceso a su computadora puede descubrir todas sus contraseñas y puede lograr el acceso a su información. Por este motivo, **siempre recuerde salir de la sesión cuando usted esté usando una computadora pública (en la biblioteca, en un cyber-café, o aún una computadora compartida en su oficina)**. Otros programas, tales como el Keychain de Apple y Secure Desktop de Palm, usan una encriptación fuerte para proteger la información. Estos tipos de programas pueden ser opciones viables para manejar sus contraseñas si encuentra que tiene demasiadas para recordar.

No hay garantía de que estas técnicas prevendrán que un atacante llegue a conocer su contraseña, pero se lo harán más difícil.

2. Consejo de Seguridad Informática ST04-005

Qué es un Software Anti-Virus

Un software anti-virus puede identificar y bloquear muchos virus antes de que éstos puedan infectar su computadora. Una vez que instale un software anti-virus, es importante mantenerlo actualizado.

¿Qué hace un software anti-virus?

Aunque hay detalles que pueden variar entre paquetes, un software anti-virus escanea los archivos en la memoria de su computadora buscando ciertos patrones que puedan indicar una infección. Los patrones que busca están basados en firmas, o definiciones, o virus conocidos. Los autores de los virus están continuamente liberando virus nuevos y actualizados, por lo tanto es importante que usted tenga las últimas definiciones instaladas en su computadora.

Una vez que usted ha instalado un paquete anti-virus, debería escanear toda su computadora periódicamente.

- **Escaneos automáticos** – Dependiendo del software que elija, puede configurarlo para que escanee automáticamente archivos y directorios específicos y le solicite a intervalos determinados que complete los escaneos.
- **Escaneos manuales** – También es una buena idea escanear manualmente archivos que recibe de una fuente externa antes de abrirlos. Esto incluye:
    - Guardar y escanear adjuntos de correo electrónico o bajadas de la web en lugar de seleccionar la opción de abrirlos directamente desde la fuente
    - Medios de escaneo, incluyendo CDs, DVDs y pendrives, para virus antes de abrir cualquiera de los archivos

¿Qué ocurre si el software encuentra un virus?

Cada paquete tiene su propio método de respuesta cuando localiza un virus, y la respuesta puede variar si el software localiza el virus durante un escaneo automático o uno manual. A veces el software abrirá una ventana de diálogo alertándolo de que encontró un virus y preguntándole si quiere que "limpie" el archivo (para sacar el virus). En otros casos, el software puede intentar eliminar el virus sin preguntarle a usted primero. Cuando usted selecciona un paquete de anti-virus, familiarícese con sus características para saber qué espera de él.

¿Qué software debería usar?

Hay muchos proveedores que producen software anti-virus, y decidir cuál elegir puede ser confuso. Todos los software anti-virus realizan la misma función, por lo tanto su decisión puede estar influenciada por las recomendaciones, características particulares, disponibilidad, o precio.

Instalar cualquier software anti-virus, independientemente de qué paquete elija, aumenta su nivel de protección. Tener cuidado, sin embargo, con los mensajes de correo electrónico que dicen incluir un software anti-virus. Estos mensajes, supuestamente provenientes del departamento de soporte técnico de su PSI, contienen adjuntos que dicen ser un software anti-virus. Sin embargo, el adjunto mismo es realidad un virus, por lo tanto usted podría infectar su máquina abriéndolo.

¿Cómo obtener la información sobre el virus actual?

Este proceso puede variar dependiendo del producto que elija, por lo tanto averigüe lo que su software anti-virus requiere. Muchos paquetes de anti-virus incluyen una opción de recibir automáticamente definiciones actualizadas de virus. Como se agrega nueva información frecuentemente, es una buena idea aprovechar esta opción. Resístase a creer en las cadenas de cartas de correo electrónico que dicen que un proveedor de anti-virus conocido recientemente ha detectado el "peor virus de la historia" que destruirá el disco duro de su computadora. Estos correos electrónicos

generalmente son engaños (*hoaxes*). Usted puede confirmar la información sobre el virus a través de su proveedor de anti-virus o a través de fuentes ofrecidas por otros proveedores de anti-virus.

Aunque instalar un software anti-virus sea una de las formas más fáciles y más efectivas de proteger su computadora, tiene sus limitaciones. Debido a que depende de firmas, el software anti-virus sólo puede detectar virus que tengan firmas instaladas en su computadora, por lo tanto es importante mantener estas firmas actualizadas. Usted será susceptible de virus que circulan antes de que los proveedores de anti-virus agreguen estas firmas, por lo tanto siga tomando otras precauciones de seguridad también.

3. Consejo de Seguridad Informática ST04-004

Saber qué son los Firewalls

Cuando cualquier persona o cosa pueda acceder a su computadora en cualquier momento, su computadora es más susceptible de ser atacada. Con un firewall usted puede resistir un acceso externo a su computadora y a la información contenida en ella.

¿Qué hacen los firewalls?

Los firewalls ofrecen protección contra atacantes externos protegiendo a su computadora o red del tráfico de Internet innecesario o malicioso. Los firewalls pueden ser configurados para bloquear datos desde ciertos lugares mientras que permiten que pasen los datos importantes y necesarios. Son especialmente importantes para los usuarios que confían en las conexiones "siempre conectado" tal como cable o modems DSL.

¿Qué tipo de firewall es el mejor?

Los firewalls se ofrecen en dos formas: hardware (externo) y software (interno). Mientras que ambos tienen ventajas y desventajas, la decisión de usar un firewall es mucho más importante que decidir qué tipo usar.

- **Hardware** – Típicamente llamados firewalls de red *(network firewalls*), estos dispositivos externos están ubicados entre su computadora o red y su cable o DSL modem. Muchos proveedores y algunos PSI (proveedores de servicio de Internet) ofrecen dispositivos llamados "routers" que también incluyen características de firewall. Los firewalls basados en hardware son particularmente útiles para proteger varias computadoras pero también ofrecen un alto grado de protección para una sola computadora. Si usted tiene sólo una computadora detrás del firewall, o si está seguro que todas las computadoras de la red están actualizadas en cuanto a parches y están libres de virus, gusanos u otro código malicioso, tal vez no necesite protección extra

de un software de firewall. Los firewalls basados en hardware tienen la ventaja de ser dispositivos separados que corren sus propios sistemas operativos, por lo tanto ofrecen una línea adicional de defensa contra ataques.

- **Software** – Algunos sistemas operativos incluyen un firewall incorporado; si el suyo lo tiene, considere habilitarlo para agregar otra capa de protección aún si usted tiene un firewall externo. Si no tiene un firewall incorporado, puede obtener un firewall de software a un bajo pequeño o sin costo de su proveedor de computadoras, proveedores de software, o PSI. Debido a los riesgos asociados con bajar software desde Internet a una computadora no protegida, lo mejor es instalar el firewall desde un CD o DVD. Si usted baja software de Internet, asegúrese que sea un sitio web de reputación y seguro. Aunque confiar en un solo firewall de software da protección, tenga en cuenta que tener el firewall en la misma computadora que la información que está tratando de proteger puede entorpecer la habilidad del firewall para atrapar el tráfico malicioso antes de que entre en su computadora.

¿Cómo saber qué tipo de configuración aplicar?

Los productos de firewall más comercialmente disponibles, tanto basados en hardware y software, vienen configurados en una forma que es aceptablemente segura para la mayoría de usuarios. Como cada firewall es diferente, usted necesitará leer y entender la documentación que viene con él para determinar si los valores de configuración por default que vienen con el firewall son suficientes para sus necesidades. Se puede obtener asistencia adicional de su proveedor de firewall o su PSI (ya fuere desde el soporte técnico o un sitio web). También, las alertas acerca de virus o gusanos corrientes a veces incluyen información acerca de restricciones que usted puede implementar a través de su firewall.

Desafortunadamente, mientras que los firewalls bien configurados pueden ser efectivos para bloquear algunos ataques, no se engañe en un falso sentido de seguridad. Aunque ellos realmente ofrecen un cierto grado de protección, los firewalls no garantizan que su computadora no será atacada. En particular, un firewall ofrece desde poco a nada de protección contra los virus que trabajan cuando los hace correr el programa infectado en su computadora, como lo hacen muchos virus que vienen en el correo electrónico. De todos modos, usar un firewall junto con otras medidas de protección (tales como software anti-virus y prácticas de computación "seguras") fortalecerán su resistencia a los ataques.

4. Consejo de Seguridad Informática ST06-009

Coordinación de Defensa contra Virus y Spyware

Usar software anti-virus y anti-spyware es una parte importante de la seguridad informática. Pero con la intención de protegerse, usted puede causar problemas sin intencionalidad.

¿No es mejor tener más protección?

Los spyware y los virus pueden interferir con la habilidad que tiene su computadora para procesar información o puede modificar o destruir datos. Usted puede sentir que cuanto más programas anti-virus y anti-spyware instale en su computadora, más seguro estará. Es cierto que no todos los programas son igualmente efectivos, y no detectarán el mismo código malicioso. Sin embargo, instalando múltiples programas en el intento de atrapar todo, puede estar introduciendo problemas.

¿Cómo pueden causar problemas los software anti-virus o anti-spyware?

Es importante usar software anti-virus y anti-spyware. Pero demasiados o del tipo incorrecto pueden afectar el funcionamiento de su computadora y la efectividad del software mismo.

El escaneo de su computadora para detectar virus y spyware usa parte de la memoria disponible de su computadora. Si usted tiene múltiples programas tratando de escanear al mismo tiempo, puede estar limitando la cantidad de recursos que quedan para realizar las tareas. Esencialmente, usted ha creado una negación de servicio contra usted mismo. También es probable que en el proceso de escaneo de virus y spyware, el software anti-virus o el anti-spyware puedan interpretar incorrectamente las definiciones de virus de otros programas. En lugar de reconocerlos como definiciones, el software puede interpretar las definiciones como un código malicioso real. Esto no sólo podría traer aparejado falsos positivos para la presencia de virus o spyware, sino que el software anti-virus o anti-spyware pueden en realidad poner en cuarentena o eliminar otro software.

¿Cómo puede evitar estos problemas?

- **Investigar sus opciones de antemano** – Investigue sobre los software anti-virus y anti-spyware disponibles para determinar la mejor elección para usted. Considere la cantidad de código malicioso que el software reconoce, y trate de encontrar con qué frecuencia se actualizan las definiciones de virus. También verifique si se conocen temas de compatibilidad con otro software que usted pueda estar corriendo en su computadora.
- **Limitar la cantidad de programas que instala** – Muchos proveedores ahora están liberando paquetes que incorporan las capacidades de anti-virus y anti-spyware juntas. Sin embargo, si usted decide elegir programas separados, en realidad sólo necesita un programa anti-virus y un programa anti-spyware. Si instala más, incrementa el riesgo de tener problemas.
- **Instalar el software en fases** – Instalar primero el software anti-virus y probarlo durante unos pocos días antes de instalar el software anti-spyware. Si surgen problemas, tiene una mejor chance de aislar la fuente y luego determinar si es un tema del software en sí mismo o con la compatibilidad.
- **Observar que no surjan problemas** – Si su computadora comienza a procesar requerimientos más lentamente, si está viendo mensajes de error cuando actualiza sus definiciones de virus, si su software no parece reconocer el código

malicioso, o si surgen otros temas que no pueden explicarse fácilmente, verifique su software anti-virus y anti-spyware.

5. Consejo de Seguridad Informática ST06-002

Desacreditar Algunos Mitos Comunes

Hay algunos mitos comunes que pueden tener influencia sobre sus prácticas de seguridad online (entendiéndose como "online" a "conectado a Internet"). Conocer la verdad le permitirá tomar mejores decisiones acerca de cómo protegerse.

¿Cómo se establecen estos mitos?

No hay una causa única para estos mitos. Pudieron haber sido gestados debido a falta de información, una suposición, conocimiento de un caso específico que fue generalizado, o alguna otra fuente. Como con cualquier mito, éstos pasan de una persona a otra, generalmente porque parecen suficientemente legítimos como para ser verdaderos.

¿Por qué es importante conocer la verdad?

Mientras que creer en estos mitos puede no presentar una amenaza directa, puede hacer que usted esté más distendido acerca de sus hábitos de seguridad. Si usted no es diligente acerca de su propia protección, puede estar más expuesto a ser una víctima de un ataque.

¿Cuáles son algunos mitos comunes, y cuál es la verdad detrás de ellos?

- *Mito: Los software anti-virus y firewalls son 100% efectivos.*
  Verdad: el software anti-virus y los firewalls son elementos importantes para proteger su información. Sin embargo, ninguno de estos elementos tienen la garantía de protegerlo contra un ataque. La mejor forma de reducir su riesgo es combinar estas tecnologías con buenas prácticas de seguridad.
- *Mito: Una vez instalado un software en su computadora, no tiene que preocuparse sobre él nunca más.*
  Verdad: Los proveedores pueden lanzar parches o versiones actualizadas de software apuntando a problemas o arreglar vulnerabilidades. Usted debería instalar los parches lo antes posible; algunos software aún ofrecen la opción de obtener actualizaciones automáticamente. Es especialmente importante que usted se asegure que tiene las últimas definiciones de virus para su software anti-virus.
- *Mito: No hay nada importante en su máquina, por lo tanto no necesita protegerla.*
  Verdad: Su opinión acerca de lo que es importante puede diferir de la opinión

del atacante. Si usted tiene información personal o financiera en su computadora, los atacantes pueden recolectarla y usarla para su propio provecho financiero. Aún si usted no almacena ese tipo de información en su computadora, un atacante que puede ganar control de su computadora y puede usarla en ataques contra otra gente.

- *Mito: Los atacantes sólo apuntan a gente con dinero.*
  Verdad: Cualquiera puede pasar a ser una víctima de robo de identidad. Los atacantes buscan la mejor recompensa por la menor cantidad de esfuerzo, por lo tanto generalmente apuntan a bases de datos que almacenan información acerca de mucha gente. Si ocurre que su información está en una base de datos, podría ser levantada y utilizada con fines maliciosos. Es importante prestar atención a su información sobre el saldo bancario para poder minimizar cualquier daño potencial.
- *Mito: Cuando las computadoras se ponen lentas, significa que son viejas y deben ser reemplazadas.*
  Verdad: Puede ser que correr programas de software más nuevos o más grandes en una computadora más vieja pudiera traer aparejado un funcionamiento lento, pero usted sólo puede necesitar reemplazar o modernizar un componente en particular (memoria, sistema operativo, drive para CD o DVD, etc.). Otra posibilidad es que haya otros procesos o programas corriendo detrás. Si su computadora se puso lenta abruptamente, usted puede estar experimentando un ataque de denegación de servicio o tener spyware en su máquina.

6. Consejo de Seguridad Informática ST04-003

Buenos Hábitos de Seguridad

Hay algunos hábitos simples que usted puede adoptar que, si los realiza consistentemente, pueden reducir dramáticamente las chances de que la información en su computadora se perdiera o se corrompiera.

¿Cómo minimizar el acceso que otra gente tiene a su información?

Usted puede identificar fácilmente a gente que podría, legítimamente o no, ganar acceso *físico* a su computadora —miembros de la familia, compañeros de habitación, compañeros de trabajo, miembros de un equipo de limpieza, y también otros. Identificar a la gente que podría ganar acceso *remoto* a su computadora se torna mucho más difícil. Siempre que usted tenga una computadora y la conecte a una red, usted es vulnerable a alguien o alguna otra cosa que acceda o corrompa su información; sin embargo, puede desarrollar hábitos para hacer esto más difícil.

- **Bloquear su computadora cuando está lejos de ella.** Aún si usted se aleja de su computadora durante unos pocos minutos, es tiempo suficiente para que

alguien destruya o corrompa su información. Al bloquear su computadora previene que otra persona pueda sentarse en su computadora y acceder a toda su información.

- **Desconectar su computadora de Internet cuando no la está usando.** El desarrollo de tecnologías tales como DSL y cable modems hicieron posible que usuarios estén todo el tiempo online (entendiéndose como "online" a "conectado a Internet"), pero esta comodidad a veces viene acompañada de riesgos. La probabilidad de que atacantes o virus que escanean la red para buscar computadoras disponibles apunten a su computadora aumenta en gran medida si su computadora está siempre conectada. Dependiendo de qué método use para conectarse a Internet, desconectar puede abarcar deshabilitar una conexión inalámbrica, apagar su computadora o modem, o desconectar los cables. Cuando usted esté conectado, asegúrese que tiene un firewall habilitado.
- **Evaluar los valores/configuración de seguridad fijados.** La mayoría de los software, incluyendo navegadores y programas de correo electrónico, ofrecen una variedad de características que usted puede diseñar de acuerdo con sus necesidades y requerimientos. Habilitar ciertas características para incrementar la comodidad o funcionalidad pueden dejarlo más vulnerable a los ataques. Es importante examinar estos valores o configuraciones, particularmente los de seguridad, y seleccionar opciones que cumplan mejor con sus necesidades sin aumentar su riesgo. Si usted instala un parche o una nueva versión de software, o si usted escucha que algo podría afectar sus valores, vuelva a evaluar estos valores para asegurarse que aún son apropiados.

¿Qué otros pasos puede tomar?

A veces las amenazas a su información no son de otra gente sino que provienen de causas naturales o tecnológicas. Aunque no hay forma de controlar o prevenir estos problemas, usted puede estar preparado para ello y minimizar el daño.

- **Proteger su computadora contra aumentos de tensión en la electricidad o apagones breves.** Además de tener tomas de corrientes para enchufar su computadora y todos sus periféricos, algunos enchufes múltiples con interruptor protegen su computadora contra aumentos de tensión. Muchos enchufes múltiples con interruptor ahora hacen propaganda de una compensación si no protegen su computadora en forma efectiva. Los enchufes múltiples con interruptor solos no lo protegen de los apagones o cortes de electricidad breves, pero son productos que ofrecen un suministro de corriente sin interrupción cuando hay saltos de tensión o cortes. Durante las tormentas con relámpagos o trabajos de construcción que incrementan los saltos de tensión, considere apagar su computadora y desenchufarla de todas las fuentes de corriente.
- **Haga back up de todos sus datos.** Independientemente de los pasos que usted tome para protegerse, siempre habrá una posibilidad de que algo ocurra y destruya sus datos. Probablemente usted ya haya experimentado esto por lo menos una vez – y haya perdido uno más archivos debido a un accidente, un virus o gusano, un episodio natural, o un problema con su equipo. Hacer un

back up de sus datos en un CD o la red en forma regular reduce el estrés y otras consecuencias negativas como resultado de perder información importante. Determinar con qué frecuencia hacer un back up de sus datos es una decisión personal Si usted está permanentemente agregando o cambiando datos, tal vez encuentre que hacer backups semanalmente sea la mejor alternativa; si su contenido cambia ocasionalmente, puede decidir que sus backups no necesitan ser tan frecuentes. No necesita hacer back up de software que tenga en un CD-ROM o DVD-ROM – puede reinstalar el software desde el medio original si fuera necesario.

7. Consejo de Seguridad Informática ST06-008

Protección de sus Datos

Cuando hay múltiples personas que usan su computadora y/o si usted en ella almacena datos personales importantes y datos relacionados con el trabajo, es especialmente importante tomar precauciones de seguridad adicionales.

¿Por qué "más" no es mejor?

Tal vez haya un programa de software adicional incluido en un programa que usted compró. O quizás usted encontró uno gratis para bajar online. Usted puede tentarse de instalar los programas sólo porque puede, o porque piensa que debería usarlos luego. Sin embargo, aún si la fuente o el software fueran legítimos, podría haber riesgos ocultos. Y si otra gente usa su computadora, hay riesgos adicionales.

Los riesgos pasan a ser especialmente importantes si usted usa su computadora para administrar sus finanzas personales (operaciones bancarias, impuestos, pago de facturas online, etc.), almacenar datos personales importantes, o realizar actividades relacionadas con su trabajo fuera de la oficina. Sin embargo hay pasos que puede tomar para protegerse.

¿Cómo puede proteger los datos tanto personales como los relacionados con el trabajo?

- **Usar y mantener un software anti-virus y un firewall** – Protéjase contra virus y caballos Troyanos que pueden robar o modificar los datos de su propia computadora y dejarlo vulnerable usando un software anti-virus y un firewall. Asegúrese de mantener sus definiciones de virus actualizadas.
- **Escanear su computadora en forma regular para detectar spyware** – Los spyware o adware escondidos en sus programas de software pueden afectar el funcionamiento de su computadora y pueden dar a los atacantes acceso a sus datos. Use un programa anti-spyware legítimo para escanear su computadora y

saque cualquiera de estos archivos. Muchos productos anti-virus tienen incorporados la detección de spyware.

- **Mantener el software actualizado** – Instalar parches de software para que los atacantes no tomen ventaja de problemas o vulnerabilidades conocidas. Muchos sistemas operativos ofrecen actualizaciones automáticas. Si esta opción está disponible, usted debería activarla.
- **Evaluar la configuración/valores establecidos en su software** – Los valores por default de la mayoría de los software permiten todas las funcionalidades disponibles. Sin embargo, los atacantes tal vez puedan tomar ventaja de esta funcionalidad para acceder a su computadora. Es especialmente importante verificar los valores para el software que conecta a Internet (navegadores, clientes de correo electrónico, etc.). Aplicar el nivel de seguridad más alto disponible que aún le de la funcionalidad que necesita.
- **Evitar programas de software que no se usan -** No abarrote su computadora con programas de software innecesarios. Si en su computadora tiene programas que no usa, considere desinstalarlos. Además de consumir recursos del sistema, estos programas pueden contener vulnerabilidades que, si no tienen parches, pueden permitir que un atacante acceda a su computadora.
- **Considerar crear cuentas de usuario separadas** - Si hay otra gente que usa su computadora, a usted le podría preocupar que alguna otra persona pudiera accidentalmente acceder, modificar, y/o eliminar sus archivos. La mayoría de los sistemas operativos (incluyendo Windows XP y Vista, Mac OS X, y Linux) le dan la opción de crear cuentas de usuario distintas para cada usuario, y usted puede establecer el grado de acceso y privilegios para cada cuenta. También puede elegir tener cuentas separadas para su trabajo y para los temas personales. Mientras que esta acción no aislará completamente cada área, ofrecerá alguna protección adicional. Sin embargo, no protegerá a su computadora contra vulnerabilidades que le dan a un atacante privilegios administrativos. Idealmente, usted debería tener computadoras separadas para el trabajo y para uso personal; esto ofrecerá un tipo diferente de protección.
- **Establecer pautas para el uso de la computadora** – Si hay varias personas que usan su computadora, especialmente niños, asegúrese que ellos saben usar la computadora e Internet en forma segura. Establecer límites y pautas lo ayudarán a proteger sus datos.
- **Usar contraseñas y encriptar archivos importantes** – Las contraseñas y otras medidas de seguridad agregan capas de protección si se las utiliza en forma correcta. El encriptado de archivos le asegurará que las personas no autorizadas no podrán ver datos aún si tienen acceso físico a la computadora. También puede considerar opciones para un encriptado total del disco, que previene que un ladrón inicie su laptop sin una frase de contraseña. Cuando use el encriptado es importante que recuerde sus contraseñas y frases de contraseña; si se las olvidara o las perdiera, puede perder toda la información.
- **Seguir las políticas de la empresa para manejar y almacenar la información relacionada con el trabajo** – Si usa su computadora con fines laborales, asegúrese de seguir todas las políticas de la empresa para manejar y almacenar la información. Estas políticas seguramente fueron establecidas para

protección de la información con patente y datos de clientes, como así también para protegerlo a usted y a la compañía de responsabilidades en cuanto a esto. Aún si no está explícitamente establecido en la política de su empresa, usted debería evitar que otras personas, incluyendo miembros de su familia, usen una computadora que contenga información de la empresa.

- **Eliminar información importante en forma efectiva** – Simplemente borrando un archivo éste no se borra totalmente. Para asegurarse que un atacante no pueda acceder a estos archivos, asegúrese de borrar los archivos importantes en forma efectiva.
- **Siga buenos hábitos de seguridad** – Tome nota de otras precauciones y pautas de seguridad para protegerse a usted mismo y proteger su información.

8. Consejo de Seguridad Informática ST05-014

Las Advertencias del Mundo Real lo Mantienen Seguro Online

Muchas de las frases de advertencia que usted probablemente escuchó de sus padres y maestros también son aplicables para el uso de las computadoras y de Internet.

¿Por qué estas advertencias son importantes?

Como en el mundo real, la tecnología e Internet presentan peligros tanto como beneficios. Los equipos fallan, los atacantes pueden apuntarlo, y se pueden cometer errores y una evaluación no adecuada. Así como usted toma precauciones para protegerse en el mundo real, necesita tomar precauciones para estar protegido online. Para muchos usuarios, las computadoras e Internet no son familiares y atemorizan, por lo tanto es aconsejable enfocarlos de la misma manera que uno alienta a los niños a enfocar el mundo real.

¿Qué advertencias recordar?

- **No confiar en caramelos que vienen de extraños** – Encontrar algo en Internet no garantiza que sea cierto. Cualquiera puede publicar información online, por lo tanto, antes de aceptar una aseveración como un hecho o tomar una acción, verifique que la fuente sea confiable. También es fácil para los atacantes falsificar ("*spoof*") direcciones de correo electrónico, por lo tanto verifique que un correo electrónico sea legítimo antes de abrir un adjunto de un correo electrónico no esperado o de responder a una solicitud de información personal.
- **Si suena demasiado bueno para que sea cierto, probablemente lo sea** – Usted probablemente haya visto muchos correos electrónicos prometiendo recompensas fantásticas o regalos de dinero. Sin embargo, independientemente de lo que está solicitando el correo electrónico, no hay ningún extraño adinerado desesperado por enviarle dinero. Esté atento a las

grandes promesas – muy probablemente sean spam, engaños (*hoaxes*), o phishing (Suplantación de identidad). También esté alerta a las ventanas que se abren solas y las propagandas de software que se bajan gratis – pueden ser un spyware disfrazado.

- **No publicar que estará fuera de su casa** – Algunas cuentas de correo electrónico, especialmente dentro de una organización, ofrecen una opción o característica (llamada un auto-contestador) que le permite crear un mensaje de "que está afuera" si usted estará fuera de su correo electrónico durante un largo período de tiempo. Este mensaje es automáticamente enviado a cualquier que le envíe un correo electrónico mientras que el auto-contestador esté habilitado. Aunque ésta es una opción útil para que sus contactos sepan que usted no podrá responder rápidamente, tenga cuidado cómo escribe su mensaje. Usted no querrá permitir que potenciales atacantes sepan que no está en su casa, o peor, darles información específica acerca de su lugar e itinerario de vacaciones. Hay opciones más seguras que incluyen frases tales como "No tendré acceso al correo electrónico entre [fecha] y [fecha]." Si fuere posible, también restrinja los receptores de su mensaje a las personas dentro de su organización o en su agenda. Si su mensaje de que estará afuera le responde a los spam, sólo confirma que su cuenta de correo electrónico está activa. Esto puede aumentar la cantidad de spam que usted recibe.
- **Bloquear lo que considere valioso** – Si un atacante puede acceder a sus datos o información personal, también podrá comprometer o robar la información. Tome los pasos necesarios para proteger esta información siguiendo buenas prácticas de seguridad. Algunas de las precauciones más básicas incluyen bloquear su computadora cuando se aleja de ella; usar firewalls y software anti-virus, y contraseñas fuertes; instalar parches adecuados; y tomar precauciones cuando navegue en Internet o use el correo electrónico.
- **Tener un plan de backup** – Como usted puede perder información o ésta puede estar comprometida (debido a un mal funcionamiento de su equipo, un error, o un ataque), haga backups de su información en forma regular para que aún así pueda tener copias limpias y completas. Los backups también lo ayudan a identificar qué cambió o qué se perdió. Si su computadora fue infectada, es importante sacar la infección antes de reiniciar el trabajo. Recuerde que si usted no se dio cuenta que su computadora estaba infectada, sus backups también pueden estar comprometidos.

9. Consejo de Seguridad Informática ST05-002

Mantener a los Niños Seguros Online (conectados a Internet)

Los niños presentan riesgos de seguridad únicos cuando usan una computadora – no sólo los tiene que mantener seguros, sino que usted tiene que proteger la información y datos de su computadora. Tomando algunos pasos simples, puede reducir las amenazas en forma alarmante.

¿Qué riesgos únicos están asociados con los niños?

Cuando un niño está usando su computadora, las protecciones y prácticas de seguridad normales pueden no ser suficientes. Los niños presentan desafíos adicionales debido a sus características naturales: inocencia, curiosidad, deseo de independencia, y miedo al castigo. Necesita considerar estas características cuando determine cómo proteger sus datos y al niño.

Usted puede pensar que como el niño sólo está jugando, o buscando un trabajo para el colegio, o tipeando un deber para el hogar, no puede causar ningún daño. ¿Pero qué ocurre si cuando el niño guarda el trabajo elimina un archivo de programa necesario? O si sin intención visita una página web maliciosa que infecta su computadora con un virus? Éstos son sólo dos escenarios posibles. Ocurren errores, pero el niño no se da cuenta de lo que hizo o puede no contarle lo que ocurrió por temor a ser retado.

Los predadores online presentan otra amenaza significativa, particularmente para los niños. Debido a que la naturaleza de Internet es tan anónima, es fácil que gente falsee su identidad y manipule o engañe a otros usuarios. Los adultos a menudo caen como víctimas de estos engaños o tácticas, y los niños, que generalmente son más abiertos y confían más, son objetivos aún más fáciles. La amenaza es aún mayor si el niño tiene acceso al correo electrónico o a programas de mensaje instantáneo, visitas a salas de chat, y/o usa sitios de red social.

¿Qué es lo que usted puede hacer?

- **Estar involucrado** - Considerar actividades sobre las que puede trabajar junto con el niño, ya fuere en un juego, buscando un tema del que han estado hablado (por ejemplo, lugares de vacaciones para la familia, un hobby en particular, un personaje histórico), o hacer un boletín de noticias familiares. Esto le permitirá supervisar las actividades online del niño mientras que le enseña buenos hábitos para la computadora.
- **Mantener su computadora en un área abierta** – Si su computadora está en un área de alto tráfico, usted podrá monitorear fácilmente la actividad de la computadora. Esta accesibilidad no sólo frenará a un niño de hacer algo que sabe que no está permitido hacer, sino que también le dará la oportunidad de intervenir si advierte una conducta que podría tener consecuencias negativas.
- **Establecer reglas y advertir sobre los peligros** – Asegúrese que su hijo conoce los límites de lo que tiene permitido hacer en la computadora. Estos límites deberían ser los adecuados para la edad, conocimiento y madurez del niño, pero deben incluir reglas acerca de cuánto tiempo tiene permitido estar en la computadora, qué sitios tiene permitido visitar, qué programas de software puede usar, y qué tareas o actividades tiene permitido hacer. También debería hablar con los niños acerca de los peligros de Internet para que reconozcan las conductas o actividades sospechosas. El objetivo no es asustarlos, si no que estén más alertas.
- **Monitorear la actividad de la computadora** - Esté al tanto de lo que su hijo esté haciendo en la computadora, incluyendo qué sitios web está visitando. Si

está usando el correo electrónico, mensaje instantáneo o salas de chat, trate de tener conocimiento de las personas con las que se contacta o si en realidad las conoce.

- **Mantener las líneas de comunicación abiertas** – Permita que su hijo sepa que se puede acercar a usted con cualquier pregunta o preocupación acerca de conductas o problemas que pudo haber encontrado en la computadora.
- **Considerar particionar su computadora en cuentas separadas** – La mayoría de los sistemas operativos (incluyendo Windows XP, Mac OS X, y Linux) le dan la opción de crear una cuenta distinta de usuario para cada usuario. Si está preocupado porque su hijo accidentalmente pueda tener acceso, modificar, y/o eliminar sus archivos, le puede dar una cuenta separada y bajar el grado de acceso y cantidad de privilegios que tiene.

  Si no tiene cuentas separadas, necesita tener especial cuidado acerca de los valores/configuración de seguridad fijados. Además de limitar la funcionalidad dentro de su navegador, evite permitir que su navegador recuerde contraseñas y otra información personal. También es siempre importante mantener sus definiciones actualizadas.

- **Considerar la implementación de controles de los padres** - Usted puede fijar algunos controles dentro de su navegador para su hijo. Por ejemplo, Internet Explorer le permite restringir o permitir que se visiten ciertos sitios web en su computadora, y usted puede proteger estos valores con una contraseña. Para encontrar esas opciones, cliquear **Herramientas** (**Tools)** en su barra de menú, seleccionar **Opciones de Internet ... (Internet Options)**, elegir la solapa **Contenido (Content)**, y cliquear el botón **Permitir ...** (**Enable)** debajo de **Asesor de Contenido** (**Content Advisor)**.

  Hay otros recursos que usted puede usar para controlar y/o monitorear la actividad online de su hijo. Algunos PSI ofrecen dispositivos diseñados para proteger a niños online. Contacte a su PSI para ver si algunos de estos servicios están disponibles. También hay programas de software especiales que usted puede instalar en su computadora. Distintos programas ofrecen distintas características y capacidades, por lo tanto puede encontrar uno que mejor se adapte a sus necesidades. Los siguientes sitios web ofrecen listados de software, y también otra información útil acerca de la protección de los niños que están online:

  - **GetNetWise** - http://kids.getnetwise.org/ - Cliquear **Tools for Families** (**Herramientas para Familias)** para llegar a la página que le permite buscar un software basado en características tales como qué hace la herramienta y qué sistema operativo usted tiene en su computadora.
  - **Yahooligans! Parents' Guide** - http://yahooligans.yahoo.com/parents/ - Cliquear **Blocking and Filtering** (**Bloqueo y Filtrado)** bajo **Related Web Sites** (**Sitios Web Relacionados**) en la barra lateral izquierda para llegar a la lista de software.