Consejos y Pautas para la Seguridad Informática (Cyber Security Tips)

Estos consejos y pautas para la Seguridad Informática describen y ofrecen asesoramiento acerca de temas de seguridad que son comunes para los usuarios de computadoras que no son técnicos.

Sistema Nacional de Alerta Informática -1° Entrega

Información General

1. Consejo de Seguridad Informática ST04-001

¿Por qué la Seguridad Informática es un problema?

Usted habrá escuchado diversas noticias acerca del robo de números de tarjetas de crédito y la propagación de virus de correos. Tal vez usted mismo ha sido una víctima. Una de las mejores defensas es conocer y comprender los riesgos, qué significan algunos de los términos básicos, y qué puede hacer para protegerse contra ellos.

¿Qué es la seguridad informática?

Pareciera que ahora todo dependiera de las computadoras e Internet - comunicación (correos electrónicos, teléfonos celulares), entretenimiento (cable digital, mp3s), transporte (sistemas de motores de automóviles, navegación en aviones), compras (negocios online, tarjetas de crédito), medicina (equipamiento, registros médicos), y la lista sigue. ¿En qué medida la mayor parte de su vida depende de las computadoras? ¿Qué volumen de su información personal está almacenado ya fuere en su propia computadora o en el sistema de otra persona?

La seguridad informática abarca proteger esa información previniendo, detectando y respondiendo a los ataques.

¿Cuáles son los riesgos?

Hay muchos riesgos, algunos más serios que otros. Entre ellos están los virus que borran todo el sistema completo, algunos entrando en su sistema y alterando archivos, otros usando su computadora para atacar otras, o alguien que roba información de su tarjeta de crédito y hace compras no autorizadas. Lamentablemente, no hay una garantía 100% de que algunos de estos episodios no le ocurrirán, aún con las mejores precauciones, pero hay pasos que usted puede tomar para minimizar las probabilidades.

¿Qué puede hacer?

El primer paso para protegerse es reconocer los riesgos y familiarizarse con algunos de los términos asociados con ellos.

- **Hacker, atacante, o intruso** – Estos términos se aplican a la gente que busca explotar las debilidades del software y los sistemas de computación para su propio provecho. Aunque sus intenciones a veces son bastante benignas y están motivadas sólo por la curiosidad, sus acciones típicamente violan el uso que se pretende dar a los sistemas que están explotando. Los resultados pueden variar desde una mera travesura (crear un virus sin ningún impacto intencionalmente negativo) a una actividad maliciosa (robar o alterar información).
- **Código malicioso** – Un código malicioso, a veces denominado “malware”, es una amplia categoría que incluye cualquier código que pudiera ser usado para atacar su computadora. Un código malicioso puede tener las siguientes características:

- Podría requerirle que usted haga algo antes de infectar su computadora. Esta acción podría ser abrir el adjunto de un correo electrónico o ir a una página web en particular.
- Algunas formas se propagan sin intervención del usuario y típicamente comienzan explotando la vulnerabilidad de un software. Una vez que la computadora víctima se ha infectado, el código malicioso intentará encontrar e infectar otras computadoras. Este código también puede propagarse vía correo electrónico, sitios web, o software basado en una red.
- Algunos códigos maliciosos dicen ser una cosa mientras que en realidad hacen algo diferente detrás de escena. Por ejemplo, un programa que dice que acelera su computadora puede en realidad estar enviando información confidencial a un intruso remoto.

Los virus y gusanos son ejemplos de código malicioso.

- **Vulnerabilidad** – En la mayoría de los casos, las vulnerabilidades son provocadas por errores de programación en el software. Los atacantes podrían tomar ventaja de estos errores e infectar su computadora, por lo tanto es importante aplicar actualizaciones o parches para corregir las vulnerabilidades conocidas.

Esta serie de consejos de seguridad le dará mayor información acerca de cómo reconocer y protegerse de los ataques

2. Consejo de Seguridad Informática ST05-013

Pautas para Publicar Información Online

Recuerde que Internet es una fuente pública. Evite publicar algo online que usted no quiere que el público vea o algo de lo que usted luego pueda querer retractarse.

¿Por qué es importante recordar que Internet tiene carácter público?

Debido a que Internet es tan accesible y contiene una abundancia de información, pasó a ser una fuente para la comunicación, para la búsqueda de temas, y para encontrar información acerca de personas. Puede parecer menos atemorizante que interactuar realmente con otras personas porque hay un sentido de anonimato. Sin embargo, usted no es realmente anónimo cuando está online, y es tan fácil para la gente encontrar información acerca de usted como para usted encontrar información acerca de ellos. Lamentablemente, mucha gente pasó a sentirse tan familiar y cómoda con Internet que puede adoptar prácticas que la hacen vulnerable. Por ejemplo, aunque a la gente típicamente le preocupa compartir información con extraños que se encuentran por la calle, puede no dudar en publicar esa misma información online. Una vez que esa información está online, un mundo de extraños puede acceder a la misma, y usted no tiene idea de lo que podrían hacer con esa información.

¿Qué pautas puede seguir usted cuando publica información en Internet?

- **Ver a Internet como una novela, no como un diario o agenda personal** – Asegúrese que usted se siente cómodo con cualquiera que está viendo la información que usted publicó online. Tenga en cuenta que gente que usted nunca conoció encontrará su página; aún si usted

mantiene un diaro o blog online, escriba en él con la expectativa de que estará disponible para el consumo del público. Algunos sitios pueden usar contraseñas u otras restricciones de seguridad para proteger la información, pero estos métodos generalmente no son utilizados

para la mayoría de los sitios web. Si usted quiere que la información sea privada o restringida a un pequeño y selecto grupo de gente, Internet probablemente no sea el mejor foro.

- **Tener cuidado con lo que anuncie o publique** - En el pasado, era difícil encontrar información acerca de alguien que no fuera su número de teléfono o domicilio. Ahora, hay una cantidad creciente de información personal disponible, especialmente porque la gente está creando páginas web personales con información acerca de ellos mismos. Cuando decida cuánta información revelar, tome conciencia de que la está transmitiendo al mundo. Dar su dirección de correo electrónico puede incrementar la cantidad de spam que reciba. Si suministra detalles acerca de sus hobbies, su trabajo, su familia y amigos, y su pasado puede darle a sus atacantes información suficiente para que hagan una ingeniería de ataque social con éxito.
- **Tomar conciencia de que no puede volver atrás** – Una vez que publica algo online, está disponible para otra gente y para los buscadores. Usted puede cambiar o sacar información luego de que algo ha sido publicado, pero es posible que alguien ya haya visto la versión original. Aún si trata de sacar información de una página o páginas de Internet, alguien pudo haber guardado una copia de la página o haber utilizado extractos en otra fuente. Algunos buscadores hacen copias "caché" de páginas para que se abran más rápido; estas copias “en cache” pueden estar disponibles aún luego de que una página web haya sido eliminada o alterada. Algunos navegadores de la web pueden también mantener un caché de las páginas web que un usuario visitó, de modo tal que la versión original puede estar almacenada en un archivo temporal o en la computadora del usuario. Piense acerca de estas consecuencias antes de publicar información – una vez que algo ya está ahí, usted no puede garantizar que puede sacarla de ahí totalmente.

Como práctica general, deje que su sentido común guíe sus decisiones acerca de lo que publique online. Antes de publicar algo en Internet, determine qué valor le da y considere las consecuencias de tener información disponible para el público. El robo de identidad es un problema que va creciendo, y cuanta mayor información el atacante pueda reunir acerca de usted, le será más fácil pretender que es usted. Compórtese online de la misma forma que se portaría en su vida diaria, especialmente cuando se trate de tomar precauciones para protegerse.

3. Consejo de Seguridad Informática ST04-024

Saber qué son los PSI – Proveedores de Servicio de Internet (ISPs)

Los PSI ofrecen servicios tales como correo electrónico y acceso a Internet. Compare factores como seguridad, servicio y costo para encontrar un PSI que cumpla con todas sus necesidades.

¿Qué es un PSI?

Un PSI, o proveedor de servicio de Internet, es una empresa que da a sus clientes acceso a Internet y otros servicios web. Además de mantener una línea directa a Internet, la empresa generalmente mantiene servidores web. Suministrando el software necesario, una cuenta de usuario protegida con una contraseña y un medio para conectarse a Internet, (por ejemplo: modem, número de teléfono), los PSI ofrecen a sus clientes la capacidad de navegar en la web e intercambiar correo electrónico con otras personas. Algunos PSI también ofrecen servicios adicionales.

Los PSI pueden variar en su tamaño – algunos están operados por un individuo, mientras que otros son grandes corporaciones. También varían en su alcance – algunos sólo soportan usuarios en una ciudad en particular, mientras que otros tienen capacidades regionales o nacionales.

¿Qué servicios ofrecen los PSI?

Casi todos los PSI ofrecen correo electrónico y navegación en la web. También ofrecen diversos grados de soporte, generalmente en la forma de una dirección de correo electrónico o un soporte de línea directa de atención al cliente. La mayoría de los PSI también ofrecen web hosting, permitiendo a sus usuarios crear y mantener páginas web personales; y algunos pueden aún ofrecer el servicio de desarrollo de páginas para usted. Muchos PSI ofrecen la opción de acceso de alta velocidad a través de DSL o cable modems, y algunos aún ofrecen conecciones dial-up.

Como parte de la operación corriente, la mayoría de los PSI realizan backups de correo electrónico y archivos web. Si la habilidad para recuperar correo electrónico y archivos web files es importante para usted, verifique con su PSI si ellos pueden hacer back up de los datos; podría no estar publicado como un servicio. Además, algunos PSI pueden implementar firewalls para bloquear cierto tráfico entrante, aunque usted debería considerar esto un suplemento de sus propias precauciones de seguridad, no un sustituto.

¿Cómo elegir un PSI?

Hay miles de PSI, y generalmente es difícil decidir cuál es el más apropiado para sus necesidades. Algunos de los factores a considerar incluyen:

- **seguridad** - ¿Usted piensa que el PSI se preocupa por la seguridad? ¿Usa encriptado y SSL para proteger cualquier información que usted suministre (por ej. nombre de usuario, contraseña)?
- **privacidad** - ¿Los PSI tienen una política de privacidad publicada? ¿Usted se siente conforme con quien tiene acceso a su información y cómo ésta es manejada y utilizada?
- **servicios** - ¿Su PSI ofrece los servicos que usted quiere? ¿Estos cumplen con sus requirimientos? ¿Hay soportes adecuados para los servicios?
- **costo** – ¿El costo del PSI está a su alcance? ¿Son razonables para la cantidad de servicios que usted recibe, tanto como el nivel de esos servicios? ¿Usted está sacrificando calidad y seguridad para obtener el precio más bajo?
- **confiabilidad**- ¿Los servicios que su PSI brinda son confiables, o frecuentemente no están disponibles debido a mantenimiento, problemas de seguridad, un alto volumen de usuarios, u otros motivos? Si el PSI sabe que los servicios no estarán disponibles por un motivo en particular, ¿le comunica esta información en forma adecuada?
- **soporte al usuario** - ¿Hay métodos publicados para contactarse con el soporte al cliente? ¿Usted recibe un servicio rápido y amigable? ¿Sus horarios de disponibilidad/atención se acomodan a sus necesidades? ¿Las personas a las que consulta tienen un nivel de conocimiento adecuado?
- **velocidad** - ¿Cuán rápida es su conexión de PSI? ¿Es suficiente para acceder a su correo electrónico o navegar en Internet?
- **recomendaciones** - ¿Ha escuchado o visto evaluaciones positivas acerca del PSI? ¿Fueron realizadas por fuentes confiables? ¿El PSI presta servicio en su área geográfica? ¿Si usted tiene puntos negativos no cubiertos, éstos son factores sobre los cuales usted está preocupado?