Privacidad

1. Consejo de Seguridad Informática ST05-008

¿Cuán anónimo es usted?

Usted tal vez piensa que es anónimo mientras que navega por los sitios web, pero siempre va quedando parte de su información. Puede reducir la cantidad de información revelada acerca de usted visitando sitios legítimos, verificando las políticas de privacidad y minimizando la cantidad de información personal que suministra.

¿Qué información es recolectada?

Cuando usted visita un sitio web, hay cierta cantidad de información que es automáticamente enviada al sitio. Esta información puede incluir lo siguiente:

- **Dirección IP** – Cada computadora en Internet tiene asignada una dirección IP (Internet Protocol) específica y única. Su computadora puede tener una dirección IP estática o una dirección IP dinámica. Si tiene una dirección IP estática, nunca cambia. Sin embargo algunos PSI (proveedores de servicio de Internet) tienen un bloque de dirección y asignan una cada vez que usted se conecta a Internet – esto es una dirección IP dinámica. Usted puede determinar la dirección IP de su computadora en cualquier momento visitando www.showmyip.com
- **Nombre del dominio** - Internet se divide en dominios, y cada cuenta de usuario está asociada con uno de esos dominios. Usted puede identificar su dominio mirando al final del URL; por ejemplo, .edu indica una institución educativa, .gob indica una organización de gobierno de Argentina, .org se refiere a organización, y .com es para uso comercial. Muchos países tienen nombres de dominio específicos. La lista de los nombres de dominio activo se encuentra en Internet Assigned Numbers Authority (IANA).
- **Información sobre el software** – Una organización puede determinar qué navegador, incluyendo la versión, usted usó para acceder a su sitio. La organización también puede determinar qué sistema operativo está corriendo su computadora.
- **Visitas a páginas** - Información acerca de qué páginas visitó, cuánto estuvo en esa página, y la organización que opera el sitio web también sabe si llegó a ese sitio desde un buscador.

Si el sitio web usa cookies, la organización puede recolectar aún más información, tal como sus patrones de navegación, que incluye otros sitios que visitó. Si el lugar que usted está visitando es malicioso, los archivos en su computadora, tanto como las contraseñas almacenadas en la memoria temporaria, pueden estar en riesgo.

¿Cómo se usa esta información?

Generalmente, las organizaciones usan la información que se recolecta automáticamente para fines legítimos, tales como la generación de estadísticas acerca de sus sitios. Analizando las estadísticas, las organizaciones pueden comprender mejor la popularidad del sitio y a qué áreas de contenido se accede más. Pueden usar esta información para modificar el sitio y así tener un mejor soporte siguiendo los patrones de la gente que lo visita.

Otra forma de aplicar la información reunida acerca de los usuarios es para fines de comercialización o marketing. Si el sitio usa cookies para determinar otros sitios o páginas que usted ya visitó, puede usar esa información para promocionar ciertos productos. Los productos pueden estar en el mismo sitio o pueden ser ofrecidos por sitios asociados.

Sin embargo, algunos sitios pueden recolectar su información para fines maliciosos. Si los atacantes pueden acceder a archivos, contraseñas, o información personal en su computadora, pueden usar estos datos para su provecho. Los atacantes pueden robarle su identidad, usar y abusar de su información personal para fines financieros. Una práctica común de los atacantes es usar este tipo de información una o dos veces, luego venderla o canjearla a otra gente. La ganancia de los atacantes de la venta o canje, y la creciente cantidad de transacciones hace difícil rastrear cada actividad detrás de ellos. Los atacantes también pueden alterar la configuración de seguridad en su computadora para poder acceder y usar su computadora para otra actividad maliciosa.

¿Usted está exponiendo cualquier otra información personal?

Mientras que las cookies pueden ser un método para recolectar información, la forma más fácil para que los atacantes ganen acceso a su información personal es preguntar por ella. Representando a un lugar malicioso como si fuera uno legítimo, los atacantes pueden convencerlo de que les de su dirección, información de tarjeta de crédito, número de seguridad social, u otros datos personales.

¿Cómo puede limitar la cantidad de información recolectada acerca de usted?

- **Tener cuidado al suministrar información personal** – A menos que confíe en el sitio, no de su domicilio, contraseña o información de su tarjeta de crédito. Busque si hay indicaciones de que el sitio use SSL para encriptar su información. Aunque algunos sitios requieren que usted proporcione su número de seguridad social (por ejemplo, sitios asociados con transacciones financieras tales como préstamos o tarjetas de crédito), tenga especial cuidado al brindar esta información online.
- **Limitar las cookies** – Si un atacante puede acceder a su computadora, podría encontrar datos personales almacenados en las cookies. Usted puede no darse cuenta del grado de información almacenada en su computadora hasta que es demasiado tarde. Sin embargo, puede limitar el uso de cookies.

- **Navegar en forma segura** – Tener cuidado con los sitios web que visita; si parece sospechoso, abandónelo. También asegúrese de tomar precauciones aumentando sus valores/configuraciones de seguridad, mantener sus definiciones de virus actualizadas, y escanear su computadora para detectar spyware.

Información Adicional

- Securing Your Web Browser http://www.us-cert.gov/reading_room/securing_browser/

2. Consejo de Seguridad Informática ST04-013

Protección de su Privacidad

Antes de proporcionar una dirección de correo electrónico u otra información personal online, debe estar seguro de que se protegerá la privacidad de esa información. Para proteger su identidad y prevenir que un atacante acceda fácilmente a información adicional acerca de usted, evite proporcionar cierta información personal tal como fecha de nacimiento y número de seguridad social online.

¿Cómo sabe si su privacidad está siendo protegida?

- **Política de privacidad** – Antes de proporcionar su nombre, dirección de correo electrónico, u otra información personal en un sitio web, busque la política de privacidad de ese sitio. Esta política debería establecer cómo será usada la información y si la información será o no distribuida a otras organizaciones. Las empresas a veces comparten información con vendedores asociados que ofrecen productos relacionados o pueden ofrecer opciones de suscribirse a una lista de correo en particular. Busque si hay indicaciones de que usted está siendo agregado a listas de correo por default – no deseleccionar esas opciones puede conducir a un spam no deseado. Si no puede encontrar una política de seguridad en un sitio web, considere contactar a la empresa pare averiguar sobre la política antes de proporcionar información personal, o busque un sitio alternativo. Las políticas de seguridad a veces cambian, por lo tanto debe revisarlas periódicamente.
- **Evidencia de que su información está siendo encriptada** – Como protección para que los atacantes no capturen información, cualquier información personal proporcionada online debería ser encriptada para que la pueda leer sólo el receptor seleccionado. Muchos sitios usan SSL (*secure sockets layer*), para encriptar la información. Las indicaciones acerca de que su información será encriptada incluyen un URL que comienza con "https:" en lugar de "http:" y un ícono de un candado en la parte inferior derecha de la ventana. Algunos sitios también indican si los datos son encriptados al ser almacenados. Si los

datos son encriptados en tránsito pero no son almacenados en forma segura, un atacante pude entrar dentro del sistema del vendedor y podría acceder a su información personal.

¿Qué pasos adicionales puede tomar para proteger su privacidad?

- **Hacer operaciones con empresas confiables** – Antes de proporcionar cualquier información online, considere contestar las siguientes preguntas: ¿tiene confianza en la empresa? ¿Es una organización establecida con una reputación confiable? ¿La información del sitio sugiere que hay una preocupación por la privacidad de la información del usuario? ¿Se ofrece una información de contacto legítima?
- **No usar su dirección de correo electrónico primaria para la información que se suministra online** – Proporcionar su dirección de correo electrónico podría significar recibir spam. Si no quiere que su dirección de correo electrónico primaria sea inundada con mensajes no deseados, considere abrir una cuenta de correo adicional para uso online. Asegurarse de abrir esa cuenta en forma regular en caso que el vendedor envíe información acerca de cambios de políticas.
- **Evitar presentar información sobre tarjeta de crédito online** – Algunas empresas ofrecen un número telefónico que se puede usar para suministrar información de su tarjeta de crédito. Aunque esto no garantiza que su información no será comprometida, elimina la posibilidad de que los atacantes pueden capturarla durante el proceso de información de la misma.
- **Asignar una tarjeta de crédito para compras online** – Para minimizar el daño potencial de que un atacante gane acceso a la información de su tarjeta de crédito, considere abrir una cuenta de tarjeta de crédito sólo para uso online. Mantenga una línea de crédito mínima en la cuenta para limitar la cantidad de cargos que un atacante puede acumular.
- **Evitar usar tarjetas de débito para compras online** – Las tarjetas de crédito generalmente ofrecen cierta protección contra el robo y pueden limitar la cantidad de dinero por la cual usted será responsable. Las tarjetas de débito no ofrecen esa protección. Como los gastos son deducidos inmediatamente de su cuenta, un atacante que obtiene información de su cuenta puede vaciar su cuenta de banco antes de que usted se de cuenta.
- **Aprovechar las opciones para limitar la exposición de información privada** – Las opciones por default en ciertos sitios web se pueden elegir por conveniencia no por seguridad. Por ejemplo, evitar permitirle a un sitio web que recuerde su contraseña. Si su contraseña está guardada, su perfil y la información de su cuenta que haya proporcionado en ese sitio web estará rápidamente disponible si un atacante gana acceso a su computadora. También evaluar sus configuraciones en los sitios web usados para red social. La naturaleza de esos sitios es compartir información pero usted puede restringir el acceso a cierta información para limitar quién puede ver y qué cosas.

3. Consejo de Seguridad Informática ST04-019

Qué es el Encriptado

El encriptado de datos es una buena manera de proteger la información delicada e importante. Asegura que sólo la persona que está autorizada puede tener acceso a los datos.

¿Qué es el encriptado?

En términos muy básicos, el encriptado es una forma de enviar un mensaje en código. La única persona que puede decodificar el mensaje es la persona con la llave correcta; para cualquier persona, el mensaje tiene el aspecto de una serie de letras, números y caracteres al azar.

El encriptado es especialmente importante si usted está tratando de enviar información delicada a la que otra persona no debería poder acceder. Como los mensajes de correo electrónico se mandan por Internet y podrían ser interceptados por un atacante, es importante agregar una capa de seguridad adicional a la información sensible.

¿En qué se diferencia de las firmas digitales?

Al igual que las firmas digitales, el encriptado de llave pública utiliza software tal como PGP, convierte información con algoritmos matemáticos y se apoya sobre llaves públicas y privadas, pero hay diferencias:

- El objetivo del encriptado es la confidencialidad – ocultando el contenido del mensaje al traducirlo a un código. El objetivo de las firmas digitales es la integridad y la autenticidad – verificar al que envía el mensajes e indicando que el contenido no ha cambiado. Aunque el encriptado y las firmas digitales puedan ser utilizadas independientemente, también puede firmar un mensaje encriptado.
- Cuando firma un mensaje, usted usa su llave privada, y cualquiera que tiene una llave pública puede verificar que la firma es válida. Cuando usted encripta un mensaje, usa la llave pública para la persona a la que se lo está enviado, y la llave privada de esta persona se usa para desencriptar el mensaje. Como la gente debería mantener sus llaves privadas en forma confidencial y debería protegerlas con contraseñas, el receptor al que se enviarán estos mensajes debería ser la única persona que pueda ver la información.

¿Cómo funciona el encriptado?

1. Obtener la llave pública para la persona que usted quiere que pueda leer la información. Si obtiene la llave de un anillo de llaves público, contactar a la

persona directamente para confirmar que la serie de letras y números asociados con la llave es la huella digital correcta.
2. Encriptar el mensaje de correo electrónico usando su llave pública. La mayoría de los clientes de correo electrónico tienen una opción para realizar esto fácilmente.
3. Cuando la persona recibe el mensaje, podrá desencriptarlo.

4. Consejo de Seguridad Informática ST05-011

Borrar Archivos en Forma Efectiva

Antes de vender o descartar una computadora vieja, o de tirar un disco o CD, usted naturalmente se asegurará que ha copiado todos los archivos que necesita. También probablemente haya intentado borrar sus archivos personales para que otras personas no puedan acceder a ellos. Sin embargo, a menos que haya tomado los pasos para asegurarse que el disco rígido, el disco, o el CD estén borrados, hay gente que aún puede resucitar esos archivos.

¿A dónde van los archivos?

Cuando usted borra un archivo, dependiendo del sistema operativo y sus configuraciones, éste puede ser transferido a la papelera. Esta "área de retención " esencialmente lo protege a usted – si accidentalmente borra un archivo, lo puede recuperar. Sin embargo, usted pudo haber experimentado el pánico como consecuencia de haber vaciado la papelera prematuramente o de que un archivo pareció desaparecer por sí solo. La buena noticia es que aún si puede parecer difícil de ubicarlo, este archivo probablemente todavía esté en su máquina. La mala noticia es que aunque usted piense que ha borrado el archivo, un atacante o una persona no autorizada puede recuperarlo.

¿Cuáles son los riesgos?

Piense en la información que usted guardó en su computadora. ¿Hay información sobre sus cuentas bancarias o tarjeta de crédito? ¿Devolución de impuestos? ¿Contraseñas? ¿Datos médicos o personales? ¿Fotos personales? ¿Información delicada de la empresa? ¿Cuánta información cualquier persona podría encontrar acerca de usted o su empresa mirando los archivos de su computadora?

Dependiendo de qué tipo de información pueda encontrar un atacante, éste podría usarla con fines maliciosos. Usted podría pasar a ser una víctima de robo de identidad. Otra posibilidad es que esa información se pudiera usar en un ataque de ingeniería social. Los atacantes pueden usar la información que encuentran acerca de usted o una organización a la que usted esté afiliado, para parecer legítimo y ganar acceso a información sensible.

¿Puede borrar archivos reformateando?

Reformatear su disco rígido a CD puede borrar superficialmente los archivos, pero la información aún esté enterrada en algún lugar. A menos que esas áreas del disco sean efectivamente sobre-escritas con nuevo contenido, es posible que atacantes expertos puedan acceder a la información.

¿Cómo puede estar seguro de que su información está totalmente borrada?

Algunas personas toman medidas extremas para asegurarse que la información quedó destruida, pero estas medidas pueden ser peligrosas y tal vez no totalmente exitosas. Su mejor opción es investigar los programas de software y dispositivos hardware que dicen borrar su disco rígido o CD. Aún así, estos programas y dispositivos tienen distintos niveles de efectividad. Cuando elija un programa de software para realizar esta tarea, busque las siguientes características:

- **Los datos están escritos múltiples veces** - Es importante asegurarse que no sólo se borró la información, sino que se escribieron datos nuevos sobre ella. Agregando varias capas de datos, el programa hace que resulte difícil para los atacantes "pelar" la nueva capa. De tres a siete pasadas es bastante estándar y debería ser suficiente.
- **Uso de datos al azar** – Usando datos al azar en lugar de patrones fácilmente identificables les dificulta a los atacantes determinar el patrón y descubrir la información original que está debajo.
- **Uso de ceros en la capa final** – Independientemente de la cantidad de veces que el programa sobre-escriba los datos, buscar programas que usen ceros en la última capa. Esto agrega un nivel de seguridad adicional.

Mientras que muchos de estos programas asumen que usted quiere borrar un disco completo, hay programas que le dan la opción de borrar y sobre-escribir archivos en forma individual.

Una forma efectiva de destruir un CD o DVD es envolverlo en una toalla de papel y hacerlo añicos. Sin embargo hay otros dispositivos de hardware que borran CDs o DVDs destruyendo la superficie. Algunos de estos dispositivos en realidad lo cortan en tiras, mientras que otros perforan la superficie donde se escribe con un patrón de agujeros. Si usted decide usar uno de estos dispositivos, compare las distintas características y precios para determinar qué opción satisface mejor sus necesidades.

5. Consejo de Seguridad Informática ST05-012

Suplementar las Contraseñas

Las contraseñas son una forma común de proteger información, pero las contraseñas solas pueden no darle la seguridad adecuada. Para obtener la mejor protección, busque sitios donde se muestren formas adicionales de verificar su identidad.

¿Por qué las contraseñas no son suficientes?

Las contraseñas son efectivas como una primera capa de protección, pero son susceptibles de ser adivinadas o interceptadas por los atacantes. Usted puede aumentar la efectividad de sus contraseñas usando tácticas tales como evitar que las contraseñas estén basadas en información personal o palabras que se encuentran en el diccionario; usando una combinación de números, caracteres especiales, letras mayúsculas y minúsculas; y no compartiendo sus contraseñas con nadie. Sin embargo, a pesar de sus mejores intentos, un atacante puede obtener su contraseña. Si no estableció medidas de seguridad adicionales, un atacante puede acceder a su información personal, financiera, o médica.

¿Qué niveles de seguridad adicionales están siendo usados?

Muchas organizaciones están comenzando a usar otras formas de verificación además de las contraseñas. Las siguientes prácticas se están tornando más y más comunes:

- **Autenticación de dos factores** – Con una autenticación de dos factores, usted usa una contraseña en conjunto con otra información adicional. Un atacante que se las ingenió para obtener su contraseña no puede hacer a nada sin el segundo componente. La teoría es similar a solicitar dos formas de identificación o dos llaves para abrir una caja de seguridad. Sin embargo, en este caso, el segundo componente es comúnmente una contraseña de "un uso" que queda anulada en cuanto la usa. Aún si un atacante puede interceptar el intercambio, no podrá ganar acceso debido a que la combinación específica no será válida nuevamente.
- **Certificados web personales -** A diferencia de los certificados usados para identificar sitios web, los certificados web personales se usan para identificar a los usuarios individuales. Un sitio web que usa certificados web personales se sustenta sobre estos certificados y el proceso de autenticación de las llaves pública/privada correspondientes para verificar que usted es quien dice ser. Debido a que la información que lo identifica está “embebida” “*embedded*” dentro del certificado, no se necesita una contraseña adicional. Sin embargo, usted debería tener una contraseña para proteger su llave privada para que los atacantes no puedan ganar acceso a su llave y se presenten como que es usted. Este proceso es similar a la autenticación de dos factores, pero difiere porque la

contraseña que protege su llave privada se usa para desencriptar la información en su computadora y nunca se manda a la red.

¿Qué sucede si pierde su contraseña o certificado?

Usted se puede encontrar en una situación donde olvidó su contraseña o que ha formateado su computadora y perdió su certificado web personal. La mayoría de las organizaciones tienen procedimientos específicos para darle acceso a su información en estas situaciones. En el caso de certificados, puede necesitar solicitar a la organización que le emita uno nuevo. En el caso de las contraseñas, puede sólo necesitar un recordatorio. No importa lo que haya sucedido, la organización requiere una forma de verificar su identidad. Para hacer esto, muchas organizaciones confían en "preguntas secretas."

Cuando usted abre una nueva cuenta (correo electrónico, tarjeta de crédito, etc.), algunas organizaciones le solicitarán que les brinde una respuesta a una pregunta. Pueden hacerle esta pregunta si los contacta porque perdió la contraseña o si requiere información acerca de su cuenta por teléfono. Si su respuesta concuerda con la que ellos tienen archivada, asumirán que se están comunicando realmente con usted. Mientras que la teoría detrás de la pregunta secreta tiene un mérito, las preguntas usadas generalmente le solicitan información personal tal como el apellido de soltera de la madre, número de seguridad social, fecha de nacimiento, nombre de la mascota. Como ahora hay tanta información personal disponible online o a través de fuentes públicas, los atacantes pueden descubrir las respuestas a estas preguntas sin mucho esfuerzo.

Tenga en cuenta que la pregunta secreta realmente es justo una contraseña adicional—cuando la establezca, no tiene que brindarla como respuesta a la información real. En realidad, cuando se le pregunta por adelantado que suministre una respuesta a este tipo de pregunta que será usada para confirmar su identidad, la mejor política puede ser la deshonestidad. Elija su respuesta tal como si eligiera cualquier otra buena contraseña, guárdela en una ubicación segura, y no la comparta con nadie.

Mientras que las prácticas de seguridad adicionales le ofrecen más de una contraseña, no hay garantía de que sean totalmente efectivas. Los atacantes también pueden tener acceso a su información, y aumentando el nivel de seguridad no lo dificulta. Esté atento a estas prácticas cuando elija un banco, una empresa de tarjeta de crédito, u otra organización que tendrá acceso a su información personal. No tema preguntar qué tipo de prácticas de seguridad utiliza la organización.