Correo electrónico y comunicación

1. Consejo de Seguridad Informática ST04-023

Entender a su Computadora: Clientes de Correo electrónico

La diferencia principal entre clientes es la interfase de usuario. Independientemente del software que decida usar, siga buenas prácticas de seguridad cuando lea o envíe correos electrónicos.

¿Cómo funcionan los clientes de correo electrónico?

Toda dirección de correo electrónico tiene dos partes básicas: el nombre de usuario y el nombre del dominio. Cuando usted está enviando un correo electrónico a otra persona, el servidor de su dominio debe comunicarse con el servidor del dominio del receptor.

Por ejemplo, asumamos que su dirección de correo electrónico es *juandoe@ejemplo.com*, y la persona que usted está contactando está en *juanasmith@otroejemplo.org*. En términos muy básicos, luego que usted presiona **enviar**, el servidor que tiene el hosting de su dominio (ejemplo.com) mira la dirección de correo electrónico y luego contacta al servidor que tiene el hosting del dominio del receptor (otroejemplo.org) para hacerle saber que tiene un mensaje de alguien en ese dominio. Una vez establecida la conexión, el servidor que tiene el hosting del dominio del receptor (otroejemplo.org) entonces mira el nombre de usuario de la dirección del correo electrónico y envía el mensaje a esa cuenta.

¿Cuántos clientes de correo electrónico hay?

Hay muchos clientes de correo electrónico y servicios diferentes, cada uno con su propia interfase. Algunos están basados en la web, otros son autónomos basados en gráfico, y otros están basados en texto. Los siguientes son algunos programas correo electrónico conocidos:

Basados en la Web

- Hotmail
- Yahoo! Mail
- Gmail

Autónomos basados en gráfico

- Outlook y Outlook Express
- Thunderbird
- Pegasus

Basados en texto

- Pine

¿Cómo elige un cliente de correo electrónico?

Generalmente hay un cliente de correo electrónico incluido con la instalación de su sistema operativo, pero hay muchas otras alternativas disponibles. Esté atento al software "de fabricación casera ", porque puede no ser tan seguro o confiable como un software que está testeado y es mantenido en forma activa. Algunos de los factores cuando decida qué cliente de correo electrónico satisface mejor sus necesidades incluyen:

- **Seguridad**- ¿Usted percibe que su programa de correo electrónico le ofrece el nivel de seguridad que quiere para enviar, recibir y leer mensajes de correo electrónico? ¿Cómo maneja los adjuntos? Si se trata de información delicada, ¿tiene la opción de enviar y recibir mensajes firmados y/o encriptados?
- **Privacidad** – Si usted está usando un servicio basado en la web, ¿leyó la política de privacidad? ¿Usted sabe qué información está siendo reunida y quién accedió a ella? ¿Hay opciones para filtrar spam?
- **Funcionalidad** – ¿El software envía, recibe e interpreta los correos electrónicos apropiadamente?
- **Confiabilidad** – Para los servicios basados en la web, ¿el servidor es confiable, o frecuentemente su correo electrónico no está disponible debido a mantenimiento, problemas de seguridad o alto volumen de usuarios u otros motivos?
- **Disponibilidad** - ¿Usted necesita poder acceder a su cuenta desde cualquier computadora?
- **Facilidad de uso** - ¿Los menús y opciones son fáciles de comprender y usar?
- **Atracción visual** - ¿Encuentra que la interfaze es atractiva?

Cada cliente de correo electrónico puede tener una forma diferente de organizar los correos en borrador, enviados, guardados y eliminados. Familiarícese con el software para que pueda encontrar y almacenar fácilmente los mensajes, para no perder mensajes inadvertidamente. Una vez que haya escogido el software que quiere usar para su correo electrónico, protéjase a usted mismo y a sus contactos siguiendo buenas prácticas de seguridad .

¿Puede tener más de un cliente de correo electrónico?

Usted puede tener más de un cliente de correo electrónico, aunque pueda tener cuestiones con la compatibilidad. Para algunas cuentas de correo electrónico, tales como aquellas emitidas a través de su proveedor de servicio de Internet (PSI) o lugar de trabajo, se puede tener acceso sólo desde una computadora que tenga privilegios y configuraciones apropiados para que usted pueda acceder a ella. Usted puede usar cualquier cliente único de correo electrónico para leer aquellos mensajes, pero si tiene

más de un cliente instalado en su máquina, debería elegir uno como el suyo por default. Cuando cliquea un link de un correo electrónico en un navegador o un mensaje de correo electrónico, su computadora abrirá ese cliente de correo electrónico que usted hubiere elegido por default.

La mayoría de los proveedores le dan la opción de bajar su software de correo electrónico directamente desde sus sitios web. Asegúrese de verificar la autenticidad del sitio antes de bajar cualquier archivo, y siga otras buenas prácticas de seguridad, tal como usar un firewall y mantener un software anti-virus actualizado, para minimizar el riesgo aún más.

También puede mantener cuentas gratis de correo electrónico a través de clientes de correo electrónico basados en el navegador (e.g., Yahoo!, Hotmail, Gmail) al que puede acceder desde cualquier computadora. Como estas cuentas están mantenidas directamente en los servidores del proveedor, no interfieren con otras cuentas de correo electrónico.

2. Consejo de Seguridad Informática ST04-010

Tener Precaución con los Adjuntos de Correo Electrónico

Mientras que los adjuntos de correo electrónico son una forma popular y práctica de enviar documentos, son una fuente común de virus. Tener precaución cuando abra adjuntos, aún si parecen haber sido enviados por alguien conocido.

¿Por qué los adjuntos de correo electrónico pueden ser peligrosos?

Algunas de las características que hacen que los adjuntos de correo electrónico sean prácticos y populares son también los que los hacen una herramienta común para los atacantes:

- **El correo electrónico tiene fácil circulación** – Enviar un correo electrónico es tan simple que los virus pueden infectar rápidamente muchas máquinas. La mayoría de los virus aún ni requieren que los usuarios envíen el correo electrónico – pueden escanear la computadora de los usuarios para detectar las direcciones de correo electrónico y enviar automáticamente el mensaje infectado a todas las direcciones que encuentren. Los atacantes pueden tomar ventaja de la realidad de que la mayoría de los usuarios automáticamente confiarán y abrirán cualquier mensaje que provengan de alguien conocido.
- **Los programas de correo electrónico tratan de estar dirigidos a las necesidades de todos los usuarios** – Prácticamente cualquier tipo de archivo puede ser adjuntado a un mensaje de correo electrónico, por lo tanto los atacantes tienen más libertad con los tipos de virus que pueden enviar.

- **Los programas de correo electrónico ofrecen varias características "amigables para el usuario"** – Algunos programas de correo electrónico tienen la opción de bajar automáticamente los adjuntos de correo electrónico, que inmediatamente exponen a su computadora a cualquier virus dentro de los adjuntos.

¿Qué pasos puede tomar para protegerse a sí mismo y otros en su agenda de direcciones?

- **Estar atento a los adjuntos no solicitados, aún provenientes de gente conocida** – Sólo porque un mensaje de correo electrónico parezca que vino de su madre, abuela o jefe, no significa que fue así. Muchos virus pueden "falsificar" (*spoof*) la dirección de retorno, que hace que parezcan como el mensaje provino de otra persona. Si puede, verifique con la persona que supuestamente le envió el mensaje para asegurarse que es legítimo antes de abrir cualquier correo electrónico. Esto incluye mensajes de correo electrónico que parezcan ser de su PSI o proveedor de software y pretenda incluir parches o software anti-virus. Los PSI y proveedores de software no envían parches o software en un correo electrónico.
- **Mantener el software actualizado** – Instale 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, debería habilitarla.
- **Confiar en sus instintos** – Si un correo electrónico o un adjunto de correo electrónico parece sospechoso, no lo abra, aún si su software anti-virus indica que el mensaje está limpio. Los atacantes están constantemente liberando nuevos virus, y el software anti-virus podría no tener la firma. Como última instancia, contacte a la persona que supuestamente le envió el mensaje para asegurarse que es legítimo antes de abrir el adjunto. Sin embargo, especialmente en el caso de los re-envíos, aún mensajes enviados por una persona legítima podrían contener un virus. Si algo acerca del correo electrónico o los adjuntos lo pone incómodo, puede haber un buen motivo. No permita que su curiosidad ponga su computadora en riesgo.
- **Guardar y escanear cualquier adjunto antes de abrirlo** – Si tiene que abrir un adjunto antes de poder verificar la fuente, siga los siguientes pasos:
    1. Estar seguro que las firmas del software anti-virus estén actualizadas.
    2. Guardar el archivo en su computadora o un disco.
    3. Escanear manualmente el archivo usando su software anti-virus.
    4. Si el archivo está limpio y no parece sospechoso, seguir adelante y abrirlo.
- **Deshabilitar la opción de bajar automáticamente los adjuntos** – Para simplificar el proceso de leer los correos electrónicos, muchos programas de correo electrónico ofrecen la característica de bajar automáticamente los adjuntos. Verificar la configuración para ver si su software ofrece la opción, y asegúrese de deshabilitarlo.

- **Considerar crear cuentas separadas en su computadora** - La mayoría de los sistemas operativos le dan la opción de crear cuentas de usuario múltiples con diferentes privilegios. Considere leer sus correos electrónicos en una cuenta con privilegios restringidos. Algunos virus necesitan privilegios del "administrador" para infectar una computadora.
- **Aplicar prácticas de seguridad adicionales** – Usted puede filtrar ciertos tipos de adjuntos a través de su software de correo electrónico (antiSpam) o un firewall.

3. Consejo de Seguridad Informática ST04-007

Reducción de Spam

Spam es un efecto secundario común y generalmente frustrante de tener una cuenta de correo electrónico. Aunque usted probablemente no podrá eliminarlo, hay formas de reducirlo.

¿Qué es spam?

Spam es la versión electrónica de "correo basura." La palabra spam se refiere a los mensajes de correo electrónico no solicitado y generalmente no deseado. El spam no necesariamente contiene virus – los mensajes provenientes de fuentes legítimas pueden caer en esta categoría.

¿Cómo puede reducir la cantidad de spam?

Hay ciertos pasos que usted puede tomar para reducir significativamente la cantidad de spam que recibe:

- **No dar a conocer su dirección de correo electrónico arbitrariamente** – Las direcciones de correo electrónico pasaron a ser tan comunes que se incluye un espacio para ellas en cualquier formulario que le solicita su domicilio – aún cartas de comentarios en los restaurantes. Tiene aspecto de inofensivo, por lo tanto mucha gente las escribe en el espacio provisto para el mismo sin darse cuenta qué podría pasar con esa información. Por ejemplo, las empresas a menudo ingresan las direcciones en una base de datos para poder rastrear a sus clientes y sus preferencias. A veces estas listas se venden o comparten con otras empresas, y repentinamente usted está recibiendo correos electrónicos que nunca solicitó.
- **Verificar las políticas de privacidad** – Antes de dar su correo electrónico online, busque una política de privacidad. Los lugares con más reputación tienen un link a su política de privacidad desde cualquier formulario en el cual se le solicita presentar datos personales. Debería leer esta política antes de dar su

dirección de correo electrónico o cualquier otra información personal para conocer lo que los propietarios del sitio piensan hacer con la información.

- **Estar alerta a las opciones seleccionadas por default** – Cuando se inscribe para algunas cuentas o servicios online, puede haber una sección que le de la opción de recibir correo electrónico acerca de ciertos productos o servicios. A veces hay opciones seleccionadas por default, por lo tanto si usted no las deshabilita, podría empezar a recibir correo electrónico de esas listas también.
- **Usar filtros** – Muchos programas de correo electrónico ofrecen capacidades de filtrado que le permiten bloquear ciertas direcciones o sólo permitir correo electrónico de direcciones que estén en su lista de contacto. Algunos PSI ofrecen un "etiquetado de spam" (*spam tagging*) o servicios de filtrado, pero los mensajes legítimos mal clasificados como spam podrían ser eliminados antes de llegar a su bandeja de entrada. Sin embargo, muchos PSI ofrecen servicios de filtrado etiquetando los mensajes sospechosos por lo tanto el usuario final puede identificarlos más fácilmente. Esto puede ser útil en conjunto con las capacidades de filtrado suministradas por muchos programas de correo electrónico.
- **Informar los mensajes como spam** – La mayoría de los clientes de correo electrónico ofrecen una opción de informar que un mensaje es spam o basura. Si usted tiene esa opción, tome ventaja de ella. Al informar que los mensajes son spam o basura, lo ayuda a hacer funcionar el filtro de correo para que los mensajes no sean entregados a la bandeja de entrada. Sin embargo, verifique sus carpetas de basura o spam cada tanto para ver si mensajes legítimos fueron clasificados incorrectamente como spam.
- **No seguir los links en los mensajes de spam** – Algunos spam confían en generadores que tratan variaciones de direcciones de correo electrónico en ciertos dominios. Si cliquea un link con un mensaje de correo electrónico o respuesta a cierta dirección, usted ya está confirmando que su dirección de correo electrónico es válida. Los mensajes no deseados que ofrecen un opción de "cancelar la suscripción" (*unsubscribe*) son particularmente tentadores, pero esto a menudo es un método para reunir direcciones válidas que luego son enviadas como otro spam.
- **Deshabilitar la bajada automática de gráficos en correo HTML** – Muchas personas que envían spam mandan correo HTML con un link de archivo de gráfico que luego se usa para rastrear quién abre el mensaje de correo – cuando su cliente de correo baja el gráfico desde su servidor web, ellos saben que usted abrió el mensaje. Deshabilitar el correo HTML completamente y ver los mensajes en texto total también previene este problema.
- **Considerar abrir una cuenta adicional de correo electrónico** – Muchos dominios ofrecen cuentas de correo electrónico gratis. Si usted frecuentemente suministra su dirección de correo electrónico (para compras online, inscribirse en servicios, o incluir en algo tal como una tarjeta de comentarios), podría preferir tener una cuenta de correo electrónico secundaria para proteger su cuenta de correo electrónico primaria de cualquier spam que se pudiera generar. Usted también podría usar esta cuenta secundaria cuando publique listas de correo, sitios de redes sociales, blogs y

foros de web al público. Si la cuenta comienza a llenarse de spam, usted puede liberarse de ello y abrir una cuenta diferente.

- **Usar configuraciones de privacidad sobre los sitios de redes sociales** – Los sitios de redes sociales típicamente le permiten elegir quién tiene acceso a ver su dirección de correo electrónico. Considere esconder su cuenta de correo electrónico o cambiar las configuraciones para que sólo un pequeño grupo de gente en la que usted confía pueda ver su dirección. También, cuando usa aplicaciones en estos sitios, podría estar dándoles permiso para acceder a su información personal. Tenga cautela acerca de qué aplicaciones elije usar.
- **No mande spam a otra gente** – Sea un usuario responsable y considerado. Algunas personas consideran los re-envíos de correo electrónico como un tipo de spam, por lo tanto sea selectivo con los mensajes que redistribuye. No re-envíe todos los mensajes a todos en su agenda de direcciones, y si alguien le pide que no le re-envía mensajes, respete su pedido.

4. Consejo de Seguridad Informática ST05-009

Beneficios y Riesgos de Servicios de Correo electrónico Gratis

Aunque los servicios de correo electrónico gratis son prácticos para enviar correspondencia personal, usted no debería usarlos para enviar mensajes que contienen información delicada.

¿Cuál es el atractivo de los servicios de correo electrónico gratis?

Muchos proveedores de servicio ofrecen cuentas de correo electrónico gratis (por ejemplo, Yahoo!, Hotmail, Gmail). Estos servicios de correo electrónico típicamente le dan una interfaz de navegación para acceder a su correo. Además del ahorro de dinero, estos servicios generalmente ofrecen otros beneficios:

- **Accesibilidad** – Como usted puede acceder a su(s) cuenta(s) desde cualquier computadora, estos servicios son útiles si usted no puede estar cerca de su computadora o está en proceso de reubicación y no tiene un PSI. Aún si usted puede acceder a su cuenta de correo electrónico basada en el PSI desde un lugar remoto, poder confiar en una cuenta de correo electrónico gratis es ideal si usted está usando una computadora pública o una conexión inalámbrica compartida y le preocupa acerca de exponer información de su cuenta primaria.
- **Característica competitiva** – Con tantos de estos proveedores compitiendo por usuarios, saben que tienen que ofrecer características u opciones adicionales tales como gran capacidad de almacenamiento, filtro spam, protección contra virus, y mayor calidad de fuentes y gráficos.

- **Capacidades adicionales** – Se está tornando cada vez más común que los proveedores de servicio hagan un paquete de software o servicios adicionales (por ejemplo, mensaje instantáneo) con sus cuentas de correo electrónico gratis para atraer clientes.

Las cuentas de correo electrónico gratis también son herramientas efectivas para reducir la cantidad de spam que recibe en su dirección de correo electrónico primario. En lugar de suministrar su dirección de correo primaria cuando esté comprando online, solicitando servicios, o participando en foros online, puede establecer usar una dirección segundaria gratis.

¿Qué riesgos están asociados con los servicios de correo electrónico gratis?

Aunque los servicios de correo electrónico gratis pueden tener muchos beneficios, usted no debería usarlos para enviar información delicada. Como usted no está pagando por la cuenta, la organización puede no tener un fuerte compromiso para protegerlo contra varias de las amenazas o de ofrecerle el mejor servicio. Algunos de los elementos que usted arriesga son:

- **Seguridad** – Si su inicio de sesión (*login*), contraseña, o mensajes son enviados en formato de texto, pueden ser fácilmente interceptados. Si el proveedor de servicio le ofrece SSL encriptado, usted debería usarlo. Usted puede ver si esto está disponible buscando un "modo seguro " o remplazando el "http:" en el URL por "https:".
- **Privacidad** – Usted no está pagando por su cuenta de correo electrónico, pero el proveedor de servicio debe encontrar alguna forma de recuperar los costos de suministrarle el servicio. Una de las formas de generar ingresos es vender espacios de publicidad, pero otra es vender o negociar. Asegúrese de leer la política de privacidad del proveedor del servicio o los términos de uso para ver si su nombre, su dirección de correo electrónico, sus direcciones de correo electrónico en su agenda de direcciones, o cualquier información en su perfil tiene el potencial de ser dada a otras organizaciones. Si está considerando re-enviar su correo electrónico a una cuenta de correo electrónico gratis, verifique con su empleador primero. Usted no quisiera violar cualquier política de seguridad establecida.
- **Confiabilidad**- Aunque usted pueda acceder a su cuenta desde cualquier computadora, necesita asegurarse que la cuenta esté disponible cuando usted quiera acceder a ella. Familiarícese con los términos de servicio del proveedor del servicio para saber exactamente qué se ha comprometido a proveerle. Por ejemplo, si el servicio finaliza o su cuenta desaparece, ¿puede recuperar sus mensajes? ¿El proveedor de servicio puede darle la posibilidad de bajar mensajes que usted quiera archivar en su máquina? También, si usted está en una zona horaria diferente que la del proveedor, puede encontrar que el mantenimiento del servidor interfiere con su rutina normal de correo electrónico.

5. Consejo de Seguridad Informática ST04-008

Beneficios de CCO (Con Copia Oculta)

Aunque en muchas situaciones puede ser apropiado listar a los receptores de correo electrónico en los campos **Para:** o **CC:**, a veces usar el campo **CCO:** puede ser la opción más deseable.

¿Qué es CCO?

CCO, que significa Con Copia Oculta (BCC: Blind Carbon Copy), le permite esconder a los que reciben los mensajes de correo electrónico. Las direcciones en el campo **Para: (To:)** y **CC:** (con copia) aparecen en los mensajes, pero los usuarios no pueden ver las direcciones de las personas incluidas en el campo **CCO: (BCC:**)

¿Por qué usted quisiera usar CCO?

Hay algunas pocas razones importantes para usar CCO:

- **Privacidad** – A veces es beneficioso, y aún necesario, que los receptores de sus correos sepan si alguien más está recibiendo su mensaje de correo electrónico. Sin embargo, hay muchas instancias cuando usted quiere enviar el mismo mensaje a múltiples receptores sin permitirles que sepan quiénes más están recibiendo el mensaje. Si está enviando correo electrónico en nombre de una empresa u organización, puede ser especialmente importante mantener confidencial las listas de los clientes, miembros, o asociados. También podría querer evitar listar una dirección de correo electrónico interna en un mensaje que está siendo enviado a receptores externos.

  Otro punto a recordar es que si cualquiera de los receptores usa la función "responder a todos" para responder a sus mensajes, todos los receptores listados en los campos **Para:** y **CC:** recibirán la respuesta. Considere usar CCO si existiera un potencial de que una respuesta no sea apropiada para todos los receptores.

- **Rastreo** – Podría ser que usted quiera acceder o archivar el mensaje de correo electrónico que está enviando a otra cuenta de correo electrónico. O tal vez quiera que alguien, como el supervisor o miembro del equipo, esté al tanto del correo electrónico sin realmente involucrarlos en el intercambio. CCO le permite cumplir con estos objetivos sin publicar que lo está haciendo.
- **Respeto por sus receptores** – La gente a menudo re-envía mensajes de correo electrónico sin eliminar las direcciones de los receptores anteriores. Como resultado, los mensajes que son enviados repetidamente a muchos receptores

pueden contener largas listas de direcciones de correo electrónico. Los que envían spam y virus dentro del correo electrónico pueden reunir y luego apuntar hacia aquellas direcciones.

Para reducir el riesgo, alerte a la gente que le re-envía mensajes que use CCO para que su dirección de correo electrónico tenga menos posibilidad de aparecer en las bandejas de entrada de otra gente y que sea susceptible de ser cosechada. Para evitar pasar a ser parte del problema, además de usar CCO si usted re-envía mensajes, tómese el tiempo para eliminar las direcciones de correo electrónico dentro del mensaje. El beneficio adicional es que la gente a la que usted está enviando el mensaje apreciará no tener que recorrer todas las largas secciones de información irrelevante para llegar al mensaje real.

¿Cómo poner un mensaje de correo electrónico como CCO?

La mayoría de los clientes de correo electrónico tienen la opción de CCO unos renglones debajo del campo **Para:.** Sin embargo, a veces es una opción separada que no está listada por default. Si no lo puede ubicar, verifique en el menú de ayuda o la documentación del software.

Si quiere poner a todos los receptores en CCO y su cliente de correo electrónico no lo dejara enviar un mensaje con el campo **Para:** vacío, considere usar su propia dirección de correo electrónico en ese campo. Además de esconder la identidad de otros receptores, esta opción le permitirá confirmar que el mensaje fue enviado exitosamente.

6. Consejo de Seguridad Informática ST04-018

Saber qué son las Firmas Digitales

Las firmas digitales son la forma de verificar que un mensaje de correo electrónico es realmente de la persona que supuestamente lo envió y que no sufrió modificaciones.

¿Qué es una firma digital?

Hay diferentes tipos de firmas digitales; este consejo apunta a las firmas digitales para mensajes de correo electrónico. Usted pudo haber recibido correos electrónicos que tienen un bloque de letras y números en la parte inferior del mensaje. Aunque pueda parecer como un texto inútil o algún tipo de error, esta información es en realidad la firma digital. Para generar una firma, se usa un algoritmo matemático para combinar la información en una clave con la información en el mensaje. El resultado es una tira de letras y números que parecen al azar.

¿Por qué usaría una?

Porque es tan fácil para los atacantes y virus "falsificar" (*spoof*) direcciones de correo electrónico que a veces es difícil identificar los mensajes legítimos. La autenticidad puede ser importante para la correspondencia empresarial – si usted está confiando en alguien para suministrar o verificar información, quiere estar seguro que la información proviene de la fuente correcta. Un mensaje firmado también indica que no se hicieron cambios en el contenido desde que fue enviado; cualquier cambio rompería la firma.

¿Cómo funciona?

Antes que usted pueda comprender cómo funciona una firma digital, hay algunos términos que debería conocer:

- Llaves (*Keys*) – Las llaves se usan para crear firmas digitales. Para cada firma, hay una llave pública y una llave privada.
    - Llave privada – La llave privada es la porción de la llave que en realidad usted usa para firmar un mensaje de correo electrónico. La llave privada está protegida por una contraseña, y usted no debería dar su llave privada a nadie.
    - Llave pública – La llave pública es la porción de la llave que está disponible para otra gente. Si usted la carga en un "anillo o archivo de claves" públicas (*key ring*) o la envía a alguien, ésta es la llave que otras personas pueden usar para verificar su firma. En su llave pública también se incluye una lista de otras personas que han firmado su llave. Usted sólo podrá ver sus identidades si ya tiene las llaves públicas en su archivo de llaves.
- Archivo de llaves (*key ring*) – Un archivo de llaves contiene llaves públicas. Usted tiene un archivo de llaves que contiene las llaves de gente a quien usted ha enviado sus llaves o cuyas llaves usted obtuvo de un servidor de llave pública. Un servidor de llave pública contiene llaves de gente que ha elegido cargar sus llaves.
- Huella digital (*fingerprint*) - Cuando confirma una llave, en realidad estará confirmando una única serie de letras y números que comprende la huella digital de la llave. La huella digital es una serie diferente de letras y números que aglutina la información que aparece al pie de un mensaje de correo electrónico firmado.
- Certificados de llave (*key certificates*) – Cuando usted selecciona una llave en un anillo de llaves, usted generalmente verá el certificado de la misma, que contiene información acerca de la llave, tal como el propietario de la llave, la fecha en que se creó, y la fecha que la llave expirará.
- "Web de confianza" |(*Web of trust*) – Cuando alguien firma su llave, está confirmando que la llave le pertenece realmente. Cuantas más llaves reúna, más fuerte se tornará su llave. Si alguien ve que su llave fue firmada por otra persona de quien confía, estará más proclive a confiar en su llave. **Nota:** Sólo

porque alguien más haya confiado una llave o si usted la encuentra en un anillo o archivo de llaves, no significa que usted debería confiar en ella automáticamente. Siempre debería verificar la huella digital usted mismo.

El proceso para crear, obtener y usar llaves es bastante directo:

1. Generar una llave usando un software tal como PGP, que significa for Pretty Good Privacy, o GnuPG, que significa GNU Privacy Guard.
2. Aumentar la autenticidad de su llave haciéndola firmar por compañeros de trabajo o asociados que también tengan llaves. En el proceso de firmar su llave, ellos confirmarán que la huella digital en la llave que usted les envió le pertenece. Haciendo esto, ellos verifican su identidad y confían en su llave.
3. Cargue o suba su llave firmada a un anillo o archivo de llaves para que si alguien recibe un mensaje con su firma, pueda verificar la firma digital.
4. Firme digitalmente sus mensajes de correo electrónico salientes. La mayoría de los clientes de correo electrónico tienen una función para agregar fácilmente su firma digital a su mensaje.

Hay una variedad de mecanismos para crear firmas digitales, y estos mecanismos pueden operar en forma diferente. Por ejemplo, S/MIME no agrega un bloque de letras y números visible dentro de un mensaje, y sus firmas digitales son verificadas *indirectamente* usando una autoridad certificada en lugar de *directamente* con otros usuarios en una web de confianza. Usted puede sólo ver un ícono y observar en el mensaje que la firma fue verificada. Si obtiene un error acerca de la firma digital, trate de contactar al que envió el mensaje a través de un llamado telefónico o una dirección de correo electrónico separada que usted sabe que es válida para verificar la autenticidad del mensaje.

7. Consejo de Seguridad Informática ST04-011

Uso de Mensaje Instantáneo y Salas de Chat en Forma Segura

Aunque brindan una forma práctica de comunicarse con otras personas, hay peligros asociados con las herramientas que permiten una comunicación en tiempo real.

¿Cuáles son las diferencias entre algunas herramientas usadas para la comunicación en tiempo real?

- **Mensaje instantáneo (MI)** – Comúnmente usado para recreación, el mensaje instantáneo está pasando a tener un uso más amplio dentro de las empresas para la comunicación entre empleados. El MI, independientemente del software específico que elija, ofrece una interfaz para que las personas realicen una comunicación uno-a-uno.

- **Salas de chat** – Ya fueren públicas o privadas, las salas de chat son foros para que grupos de gente interactúen. Muchas salas de chat están basadas en una característica compartida; por ejemplo, hay salas de chat para gente de un grupo de edad o intereses en particular. Aunque la mayoría de los clientes de MI soportan "chats" entre usuarios múltiples, el MI es tradicionalmente de uno-a-uno mientras que los chats son tradicionalmente de muchos-a-muchos.
- **Bots** – Un "robot de chat," o "bot," es un software que puede interactuar con usuarios a través de mecanismos de chat, ya fuere en MI o salas de chat. En algunos casos, los usuarios pueden obtener informes meteorológicos actuales, estado de la bolsa, o listados de películas. En estos casos, los usuarios generalmente saben que no están interactuando con un humano real. Sin embargo, algunos usuarios pueden ser engañados por bots más sofisticados al pensar que las respuestas que están recibiendo provienen de otra persona.

Hay muchos paquetes de software que incorporan una o más de estas características. Se podrían soportar una cantidad de tecnologías diferentes, incluyendo MI, Internet Relay Chat (IRC), o Jabber.

¿Cuáles son los peligros?

- **Las identidades pueden ser difíciles de localizar o ambiguas** – No sólo a veces es difícil de identificar si la "persona" con la que usted está hablando es un humano, sino que la naturaleza y comportamiento humano no es predecible. La gente puede mentir acerca de su identidad, las cuentas pueden quedar comprometidas, los usuarios pueden olvidar de salir de la sesión, o una cuenta puede ser compartida por múltiples personas. Todas estas cosas hacen difícil saber con quién realmente una persona está hablando durante una conversación.
- **Los usuarios son especialmente susceptibles de ciertos tipos de ataque** – Tratar de convencer a alguien de correr un programa o cliquear un link es un método de ataque común, pero puede ser especialmente efectivo a través de MI o salas de Chat. En un escenario donde un usuario se siente cómodo con la "persona" con quien está hablando, un software malicioso o un atacante tiene más posibilidades de convencer a alguien que caiga en la trampa.
- **Usted no sabe quién más podría estar mirando la conversación** – Las interacciones online son fácilmente almacenables, y si usted está usando un servicio comercial gratis, los intercambios pueden ser archivados en un servidor. Usted no tiene control sobre lo que ocurre en esos registros. Usted tampoco sabe si hay alguien mirando por encima del hombro de la persona con la que usted está hablando, o si un atacante podría estar "olfateando" su conversación.
- **El software que usted está usando puede contener vulnerabilidades** – Como otros software, el software de chat puede tener vulnerabilidades que los atacantes pueden explotar.
- **Las configuraciones de seguridad por default pueden no ser apropiadas** - Las configuraciones de seguridad por default en el software de chat tienden a ser

relativamente permisivas para hacerlas más abiertas y "utilizables," y esto puede hacer que usted sea susceptible a los ataques.

¿Cómo se pueden usar estas herramientas en forma segura?

- **Evaluar su configuración de seguridad** – Verifique en su software las configuraciones por default y ajústelas si son muy permisivas. Asegúrese de deshabilitar los comandos de bajadas automáticas. Algunos software de chat ofrecen la habilidad de limitar las interacciones a sólo ciertos usuarios, y usted puede tomar ventaja de estas restricciones.
- **Sea consciente de qué información revela** – Esté atento con respecto a revelar información personal a menos que sepa con quién está hablando. Debería tener cuidado al discutir algo que usted o su empleador podrían considerar información comercial delicada por medio de MI o servicios de chat (aún si usted está hablando con alguien que conoce en una conversación uno-a-uno).
- **Trate de verificar la identidad de la persona con quien está hablando, si le interesa** – En algunos foros y situaciones, la identidad de la "persona" con quien usted está hablando no tiene importancia. Sin embargo, si necesita tener un grado de confianza en esa persona, ya fuere porque está compartiendo ciertos tipos de información o se le está requiriendo que tome alguna acción como seguir un link o correr un programa, asegúrese que la "persona" con quien está hablando sea realmente esa persona.
- **No crea en todo lo que lee** – La información o consejo que recibe en una sala de chat o por el MI pueden ser falsa, o peor, maliciosa. Trate de verificar la información o instrucciones desde fuentes externas antes de tomar cualquier acción.
- **Mantenga el software actualizado** – Esto incluye el software de chat, su navegador, su sistema operativo, su cliente de correo, y especialmente, su software anti-virus.

8. Consejo de Seguridad Informática ST06-003

Estar Seguro en los Sitios de Redes Sociales

La popularidad de los sitios de redes sociales continúa aumentado, especialmente entre adolescentes y adultos jóvenes. La naturaleza de estos sitios introduce riesgos de seguridad, por lo tanto usted debería tomar ciertas precauciones.

¿Qué son los sitios de redes sociales?

Los sitios de redes sociales, a veces conocidos como sitios de "amigo de un amigo", se construyen sobre el concepto de redes sociales tradicionales donde usted está conectado con gente nueva a través de gente que ya conoce. El fin de algunos sitios de

red puede ser puramente social, permitiendo a los usuarios establecer amistades o relaciones amorosas, mientras que otros pueden estar enfocados a establecer conexiones empresariales.

Aunque algunas características de los sitios de redes sociales difieren, todos permiten que usted suministre información acerca de usted mismo y que ofrezca algún tipo de sistema de comunicación (foros, salas de chat, correo electrónico, mensaje instantáneo) que le permiten conectarse con otros usuarios. En algunos sitios, usted puede navegar y buscar gente basándose en ciertos criterios, mientras que otros sitios requieren que usted sea "presentado" a gente nueva a través de una conexión que usted comparte. Muchos de los sitios tienen comunidades o subgrupos que pueden estar basados en un interés en particular.

¿Qué consecuencias en cuanto a seguridad presentan estos sitios?

Los sitios de redes sociales se sostienen sobre conexiones y comunicaciones, por lo tanto lo alientan a suministrar una cierta cantidad de información personal. Al decidir cuánta información revelar, la gente puede no poner en práctica la misma precaución que tendría cuando conoce o se encuentra con alguien en persona debido a que:

- Internet da un sentido de anonimato
- La falta de interacción física provoca una falsa sensación de seguridad
- Ellos arman la información para que sus amigos la lean, olvidándose que otros pueden verla
- Quieren ofrecer una comprensión o entendimiento para impresionar potenciales amigos y asociados

Mientras que la mayoría de la gente que utiliza estos sitios no presenta una amenaza, puede haber gente maliciosa dirigida a ellos debido a la accesibilidad y la cantidad de información personal disponible. Cuanta mayor sea la información maliciosa que la gente tenga acerca suyo, le será más fácil tomar ventaja de usted. Los depravados pueden gestar relaciones online y luego convencer a los individuos desprevenidos para encontrarlos personalmente. Esto podría llevar a una situación peligrosa. La información personal también puede ser utilizada para conducir un ataque de ingeniería social. Usando la información que usted brinda o publica acerca de su ubicación, hobbies, intereses, y amigos, una persona maliciosa podría hacerse pasar por un amigo confiable o convencerlo de que ellos tienen la autoridad de acceder a otros datos personales o financieros.

Adicionalmente, debido a la popularidad de estos sitios, los atacantes pueden usarlos para distribuir código malicioso. Los sitios que ofrecen aplicaciones desarrolladas por terceros son particularmente susceptibles. Los atacantes pueden crear aplicaciones a medida que parecieran ser inocentes mientras que están infectando su computadora sin su conocimiento.

¿Cómo puede protegerse a usted mismo?

- **Limitar la cantidad de información personal que publica** – No publique información que podría hacerlo vulnerable, tal como su domicilio o información acerca de su programa o rutina. Si sus conexiones publican información acerca suyo, asegúrese que la información combinada no excede lo que usted se sentiría cómodo de compartir con extraños. También sea considerado cuando publica información acerca de sus conexiones, incluyendo fotos.
- **Recordar que Internet es un recurso público** – Sólo publique información con la que se siente cómodo que otra gente pueda ver. Esto incluye información y fotos en su perfil y en blogs y otros foros. También, una vez que usted publica información online, no se puede retractar. Aún si usted elimina la información de un sitio, puede aún haber versiones guardadas o en caché en las máquinas de otras personas.
- **Esté atento a extraños** - Internet facilita a las personas para tergiversar sus identidades y motivos. Considere limitar la gente que tiene permitido contactarlo en estos sitios. Si usted interactúa con gente que no conoce tenga cuidado acerca de la información que revela o de acordar encuentros personalmente.
- **Sea escéptico** – No crea en todo lo que lee online. Hay gente que puede publicar información falsa o engañosa, incluyendo sus propias identidades. Esto no se hace necesariamente con intención maliciosa; podría ser no intencional, una exageración o un chiste. Tome las precauciones apropiadas y trate de verificar la autenticidad de toda información antes de tomar alguna acción.
- **Evaluar sus configuraciones** – Tome ventaja de las configuraciones de seguridad de un sitio. Las configuraciones por default para algunos sitios pueden permitir que cualquiera vea su perfil. Usted puede establecer su configuración de acuerdo con sus requerimientos para restringir el acceso sólo a ciertas personas. Sin embargo, hay un riesgo de que aún esta información privada pudiera estar expuesta, por lo tanto no publique algo que usted no quisiera que el público viera. También, tenga precaución cuando decida qué aplicaciones habilitar, verifique sus configuraciones para ver a qué información podrán acceder estas aplicaciones.
- **Usar contraseñas fuertes** – Proteja su cuenta con contraseñas que no puedan ser fácilmente adivinadas. Si su contraseña está comprometida, alguien puede tener acceso a su cuenta y pretender que es usted.
- **Verificar las políticas de privacidad** – Algunos sitios pueden compartir con otras empresas información tal como direcciones de correo electrónico o preferencias de otros usuarios. Esto puede llevar a un aumento de spam. También, trate de encontrar la política para manejar las direcciones que usted refiera a alguien, para asegurarse que no incorporó sin intención a amigos y que luego puedan recibir spam. Algunos sitios continuarán enviando mensajes de correo electrónico a cualquiera que usted haya referido, hasta que se junten.

- **Usar y mantener un software anti-virus** – El software anti-virus reconoce los virus más conocidos y protege a su computadora contra ellos, entonces usted podrá detectar y eliminar el virus antes de que haga algún daño. Debido a que los atacantes están permanentemente liberando nuevos virus, es importante mantener sus definiciones actualizadas.

Los niños son especialmente susceptibles a estas amenazas que presentan los sitios de redes sociales. Aunque muchos de estos sitios tienen una restricción de edad, los niños pueden falsear sus edades para poder unirse. Enseñando a los niños los temas de seguridad en Internet, estando atento a sus hábitos online, y guiándolos hacia los sitios apropiados, los padres pueden asegurarse que los niños serán usuarios seguros y responsables.