Navegación Segura

1. Consejo de Seguridad Informática ST04-022

Conozca su computadora: Navegadores Web

Los navegadores web le permiten navegar por Internet. Hay una variedad de opciones disponibles, por lo tanto puede elegir la que mejor satisfaga sus necesidades.

¿Cómo funcionan los navegadores web?

Un navegador web es una aplicación que encuentra y muestra páginas web. Coordina la comunicación entre su computadora y el servidor web donde "residen" un sitio web en particular.

Cuando usted abre su navegador y tipea una dirección web (URL) para un sitio web, el navegador contacta ese servidor, solicita la página web que usted pidió, y muestra la página en su computadora. El navegador traduce el código (escrito en un idioma tal como HTML o XML) para los diferentes elementos de la página (texto, imágenes, sonidos) a un formato apropiado y muestra la página resultante.

¿Cuántos navegadores existen?

Hay muchos navegadores diferentes. La mayoría de los usuarios están familiarizados con navegadores gráficos, que muestran tanto texto como gráficos y pueden también mostrar elementos multimedia tales como sonido o video clips. Sin embargo, también hay navegadores basados en texto. Los siguientes son algunos de los navegadores conocidos:

- Internet Explorer
- Firefox
- AOL
- Opera
- Safari – un navegador específicamente diseñado para computadoras Macintosh
- Lynx – un navegador basado en texto para los usuarios con discapacidad visual debido a la disponibilidad de dispositivos especiales para leer el texto

¿Cómo elegir un navegador?

Generalmente con la instalación de su sistema operativo se incluye un navegador, pero usted no está restringido a esa elección. Algunos de los factores a considerar cuando decida qué navegador se ajusta mejor a sus necesidades, necesita incluir:

- **Compatibilidad** - ¿El navegador funciona con su sistema operativo?

- **Seguridad** - ¿Considera que su navegador le ofrece el nivel de seguridad que usted quiere?
- **Fácil de usar** - ¿Los menús y opciones son fáciles de entender y usar?
- **Funcionalidad** - ¿El navegador interpreta correctamente el contenido web? ¿Si necesita instalar otros plug-ins o dispositivos para trasladar ciertos tipos de contenido, funcionan?
- **Atracción** - ¿Encuentra que la interfaz y la forma que el navegador interpreta el contenido web son visualmente atractivos?

¿Puede tener más de un navegador instalado al mismo tiempo?

Si decide cambiar su navegador o agregar otro, no tiene que desinstalar el navegador que tiene actualmente en su computadora - puede tener más de un navegador a la vez en su computadora. Sin embargo, a usted se le solicitará que elija un navegador por default. Todas las veces que siga un link en un mensaje de correo electrónico o documento, o hace doble click en un atajo a una página web en su computadora, la página abrirá usando su navegador por default. Usted puede abrir manualmente la página en otro navegador.

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

2. Consejo de Seguridad Informática ST05-001

Evaluar las Configuraciones de Seguridad de su Navegador Web

Verifique las configuraciones/valores de seguridad en su navegador web para asegurarse que están en el nivel apropiado. Mientras que incrementar su seguridad puede afectar la funcionalidad de algunos sitios web, podría prevenirlo de ser atacado.

¿Por qué son tan importantes las configuraciones/valores de seguridad para sus navegadores web?

Su navegador web es su conexión primaria al resto de Internet, y muchas aplicaciones para funcionar pueden confiar en su navegador, o elementos dentro de su navegador. Esto hace que las configuraciones de seguridad en su navegador sean aún más importantes. Muchas aplicaciones web tratan de incrementar su experiencia de navegación habilitando diferentes tipos de funcionalidad, pero esta funcionalidad podría ser innecesaria y puede dejarlo susceptible de ser atacado. La política más segura es deshabilitar la mayoría de esos valores a menos que decida que son necesarios. Si usted determina que un sitio es confiable, usted puede elegir habilitar la funcionalidad temporalmente y luego deshabilitarla una vez que terminó de visitar el sitio.

¿Dónde puede encontrar los valores/configuración?

Cada navegador web es diferente, por lo tanto tiene que buscar. Por ejemplo, en Internet Explorer, puede encontrarlos cliqueando en **Herramientas (Tools)** en la barra del menú, seleccionar **Opciones de Internet (Internet Options...)**, eligiendo la solapa de **Seguridad (Security)** y cliqueando el botón **Nivel a Medida (Custom Level...**). Sin embargo, en Firefox, cliquear en **Herramientas (Tools)** en la barra del menú y seleccionar **Opciones de Internet (Options...**.) Cliquear **Contenido (Content)**, las solapas de **Privacidad (Privacy**) y **Seguridad** (**Security)** para explorar las opciones de seguridad básicas. Los navegadores tienen distintas opciones y configuraciones de seguridad, por lo tanto familiarícese con las opciones del menú, verifique la opción de ayuda, o refiérase al sitio web del proveedor.

Mientras que toda aplicación tiene valores que están seleccionados por default, usted puede descubrir que su navegador también tiene niveles de seguridad predefinidos para seleccionar. Por ejemplo, Internet Explorer ofrece valores a medida que le permiten seleccionar un nivel de seguridad en particular; se habilitan o deshabilitan características basadas en su selección. Aún con estas guías, es útil comprender qué significan los diferentes términos para poder evaluar las características y determinar cuáles son las apropiadas para usted.

¿Cómo sabe cuáles deberían ser sus valores/configuración?

Idealmente, usted pondría su seguridad en el nivel más alto posible. Sin embargo, al restringir ciertos valores se puede limitar la bajada o buen funcionamiento de algunas páginas web. El mejor enfoque es adoptar el nivel de seguridad más alto y sólo habilitar ciertos valores cuando usted requiera sus funcionalidades.

¿Qué significan los distintos términos?

Los navegadores usan distintos términos, pero hay algunos términos y opciones que puede encontrar:

- **Zonas** - Su navegador puede darle la opción de poner sitios web en segmentos diferentes y permitirle que defina distintas restricciones de seguridad para cada zona.

  Por ejemplo, Internet Explorer identifica las siguientes zonas:

  - **Internet** - Ésta es la zona general para todos los sitios web públicos. Cuando usted navega en Internet, los valores para esta zona se aplican automáticamente a los sitios que usted visita. Para darle la mejor protección cuando usted navega, debería fijar los valores en el nivel más alto; como mínimo, debería mantener un nivel medio.
  - **Intranet local** – Si usted está en un escenario de una oficina que tiene su propia intranet, esta zona contiene aquellas páginas internas. Como el contenido web es mantenido en un servidor web interno,

generalmente es seguro tener valores menos restrictivos para estas páginas. Sin embargo, algunos virus han traspasado esta zona, por lo tanto esté atento a los sitios que están listados y qué privilegios se les está dando.

- **Sitios confiables** – Si cree que ciertos sitios están diseñados con la seguridad en mente, y siente que puede confiar en que el contenido del sitio no contiene materiales maliciosos, puede agregarlos a sus sitios confiables y aplicar los valores de acuerdo con esto. También puede requerir que sólo los sitios que implementen Secure Sockets Layer (SSL) puedan estar activos en esta zona. Esto le permite verificar que el sitio que está visitando es el sitio que dice ser. Ésta es una zona opcional pero puede ser útil si usted personalmente mantiene sitios web múltiples o si su organización tiene sitios múltiples. Aún si confía en ellos, evite aplicar niveles de seguridad bajos para los sitios externos - si son atacados, usted podría también convertirse en una víctima.
- **Sitios restringidos** – Si hay sitios en particular que usted piensa que podrían no ser seguros, puede identificarlos y definir valores de seguridad más elevados. Como los valores de seguridad pueden no ser suficientes para protegerlo, la mejor precaución es evitar navegar a cualquier sitio que pueda hacerlo dudar sobre su seguridad.

- **JavaScript** – Algunos sitios web confían en web scripts tales como JavaScript para lograr una cierta apariencia o funcionalidad, pero estos scripts pueden ser utilizados en ataques.
- **Controles Java y ActiveX** – Estos programas se usan para desarrollar o ejecutar contenido activo que da alguna funcionalidad, pero lo pueden poner en riesgo.
- **Plug-ins** – A veces los navegadores requieren la instalación de software adicional conocido como plug-ins para darle una funcionalidad adicional. Al igual que los controles Java y ActiveX, los plug-ins pueden usarse en un ataque, por lo tanto, antes de instalarlos asegúrese que son necesarios y que el sitio de donde tiene que bajarlos es confiable.

También puede encontrar opciones que le permiten tomar las siguientes medidas de seguridad:

- **Manejar las cookies** – Usted puede deshabilitar, restringir, o permitir las cookies, de acuerdo con lo que considere apropiado. Generalmente, lo mejor es deshabilitar los cookies y luego habilitarlos si visita un sitio en el que confía y que los necesita.
- **Bloquear ventanas emergentes** – Aunque habilitando esta función podría restringir la funcionalidad de ciertos sitios web, también minimizará la cantidad de ventanas emergentes que recibe, algunas de las cuales pueden ser maliciosas.

3. Consejo de Seguridad Informática ST07-001

Comprar Online en Forma Segura

Las compras online se tornaron en una forma popular de comprar objetos sin las dificultades del tránsito y amontonamiento de gente. Sin embargo, Internet tiene riesgos únicos, por lo tanto es importante tomar los pasos necesarios para protegerse cuando compre online.

¿Por qué los que compran online tienen que tomar precauciones especiales?

Internet ofrece una practicidad que no está disponible en ningún otro punto de venta. Desde el confort de su hogar, puede buscar objetos de innumerables vendedores, comparar precios con unos simples cliqueos del mouse, y hacer compras sin esperar en una fila. Sin embargo, Internet también es práctico para los atacantes, dándoles múltiples formas de acceder a información personal y financiera de compradores que no sospechan. Los atacantes que pueden obtener esta información pueden usarla para su propio provecho financiero, ya fuere haciendo compras ellos mismos, o vendiendo la información a otra persona.

¿Cómo los atacantes apuntan a los compradores online?

Hay tres formas comunes en que los atacantes pueden tomar ventaja de los compradores online:

- **Apuntando las computadoras vulnerables** – Si usted no toma acciones para proteger su computadora de virus y otro código malicioso, un atacante puede ganar acceso a su computadora y toda la información en ella. También es importante para los proveedores proteger sus computadoras para prevenir que los atacantes tengan acceso a las bases de datos de cliente.
- **Creando sitios y mensajes de correo electrónico fraudulentos** – A diferencia de las compras tradicionales, donde usted sabe que un negocio es realmente el negocio que dice ser, los atacantes pueden crear sitios web maliciosos que imitan a los legítimos o crear mensajes de correo electrónico que parecen provenir de una fuente legítima. Las organizaciones benéficas también pueden tener una representación engañosa en esta forma, especialmente luego de desastres naturales o durante la época de vacaciones. Los atacantes crean estos sitios maliciosos y mensajes de correo electrónico para tratar de convencerlo de brindar información financiera.
- **Interceptando transacciones inseguras** – Si un proveedor no usa el encriptado, un atacante puede interceptor su información cuando ella está siendo transmitida.

¿Cómo puede protegerse?

- **Usar y mantener software anti-virus, un firewall, y un software anti-spyware** – Protéjase contra los virus y los Troyanos que pueden robar y modificar los datos en su propia computadora y dejarlo vulnerable usando software anti-virus y un firewall. Asegúrese de mantener sus definiciones de virus actualizadas. Los spyware o adware escondidos en los programas de software también pueden darle a los atacantes acceso a sus datos, por lo tanto use un programa anti-spyware legítimo para escanear su computadora y sacar cualquiera de estos archivos.
- **Mantener actualizado el software, particularmente su navegador** – Instalar parches para que los atacantes no puedan conocer los problemas y vulnerabilidades. Muchos sistemas operativos ofrecen actualizaciones automáticas. Si esta opción está disponible, debería habilitarla.
- **Evaluar las configuraciones/valores de su software** – Los valores por default de la mayoría de los softwares permiten toda la funcionalidad disponible. Sin embargo, los atacantes pueden aprovechar esta funcionalidad para acceder a su computadora. Es especialmente importante verificar los valores de su 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.
- **Hacer transacciones con vendedores de reputación** – Antes de brindar cualquier información personal o financiera, asegúrese de que está interactuando con un proveedor de reputación y establecido. Algunos atacantes pueden tratar de engañarlo creando sitios web maliciosos que parecen ser legítimos, por lo tanto verifique la legitimidad antes de brindar cualquier información. Localice y anote los números de teléfono y los domicilios físicos de los vendedores en caso que hubiera un problema con su transacción o factura.
- **Aproveche los valores/configuraciones de seguridad** – Las contraseñas y otras configuraciones de seguridad agregan capas de protección si se las utiliza en forma apropiada.
- **Esté atento a los correos electrónicos que requieren información** – Los atacantes pueden intentar recolectar información enviando correos electrónicos solicitando que confirme una compra o información sobre la cuenta. Las empresas legítimas no le solicitarán este tipo de información por correo electrónico.
- **Verificar las políticas de seguridad** – Antes de brindar información personal o financiera, verificar la política de privacidad del sitio web. Asegúrese que entiende cómo su información será almacenada y usada.
- **Asegúrese que su información está siendo encriptada** – Muchos sitios usan SSL, (secure sockets layer) para encriptar información. Las indicaciones de que su información será encriptada incluyen un URL que comienza con "https:" en lugar de "http:" y un ícono de candado. Si el candado está cerrado, la información está encriptada. La ubicación del ícono varía según el navegador; por ejemplo, puede estar a la derecha de la barra de la dirección o al pie de la ventana. Algunos atacantes tratan de engañar a los usuarios agregando un

ícono de candado falso, por lo tanto asegúrese que el ícono esté en el lugar apropiado de su navegador.

- **Usar una tarjeta de crédito** – Hay leyes que limitan su responsabilidad por cargos de tarjetas de crédito fraudulentas, y usted puede no tener el mismo nivel de protección con su tarjeta de débito. Adicionalmente, debido a que la tarjeta de débito retira dinero directamente de su cuenta de banco, los cargos no autorizados podrían dejarlo sin fondos suficientes para pagar otras cuentas. Puede aún minimizar más el daño usando un sola tarjeta para todas las compras online.
- **Controlar los resúmenes de cuenta** – Mantenga un registro de sus compras y copias de las páginas de confirmación, y compárelas con los resúmenes bancarios. Si hubiera discrepancias, infórmelo inmediatamente.

4. Consejo de Seguridad Informática ST04-012

Navegar en forma Segura: Saber qué son los Contenidos Activos y Cookies

Mucha gente navega en Internet sin pensar mucho en lo que está sucediendo detrás de la escena. El contenido activo y los cookies son elementos comunes que pueden presentar riesgos ocultos cuando se los ve en un navegador o cliente de correo electrónico.

¿Qué es un contenido activo?

Para aumentar la funcionalidad y agregar embellecimientos de diseño, los sitios web a menudo confían en scripts que ejecuten los programas dentro del navegador web. Este contenido activo puede ser utilizado para crear "splash pages" (página de un sitio web que un usuario ve antes de ingresar al contenido principal) u opciones tales como menús desplegables (drop-down). Desafortunadamente, estos scripts generalmente son un medio utilizado por los atacantes para bajar o ejecutar un código malicioso en la computadora de un usuario.

- **JavaScript** - Es uno de los tantos web scripts (otros ejemplos son VBScript, ECMAScript, y JScript) y es probablemente el más reconocido. Utilizado en prácticamente todo sitio web ahora, JavaScript y otros scripts son populares porque los usuarios esperan la funcionalidad y "miran" qué suministra y es fácil de incorporar (muchos programas de software comunes para construir sitios web tienen la capacidad de agregar características de JavaScript con poco esfuerzo o conocimiento por parte del usuario). Sin embargo, por estos motivos, los atacantes pueden manipularlo para su propio fin. Un tipo de ataque popular que confía en JavaScript involucra redirigir a los usuarios de un sitio web legítimo a uno malicioso que puede bajar virus o recolectar información personal.
- **Controles Java y ActiveX** – A diferencia de JavaScript, los controles Java y ActiveX son programas reales que residen en su computadora o que pueden ser bajados de la red dentro de su navegador. Si es ejecutado por atacantes, los controles ActiveX no confiables pueden hacer en su computadora cualquier

cosa que usted pueda hacer (tal como correr un spyware y recolectar información personal, conectar a otras computadoras, y potencialmente hacer otro daño). Los *applets* Java generalmente corren en un entorno más restringido, pero si ese entorno no es seguro, entonces los *applets* Java maliciosos pueden crear oportunidades para atacar también.

Los JavaScript y otras formas de contenido activo no son siempre peligrosos, pero son herramientas comunes para los atacantes. Usted puede prevenir que el contenido activo corra en la mayoría de los navegadores, pero tenga en cuenta que el agregado de seguridad puede limitar la funcionalidad y romper las características de algunos sitios que visita. **Antes de cliquear en un link para un sitio web con el cual usted no está familiarizado o del que no confía, tome la precaución de deshabilitar el contenido activo.**

Estos mismos riesgos pueden también aplicarse al programa de correo electrónico que usa. Muchos clientes de correo electrónico usan los mismos programas que los navegadores web para mostrar HTML, por lo tanto las vulnerabilidades que afectan el contenido activo como el JavaScript y ActiveX a menudo se aplican al correo electrónico. Ver los mensajes como texto completo puede resolver este problema.

¿Qué son las cookies?

Cuando usted navega en Internet, la información de su computadora puede ser recolectada y almacenada. Esta información podría ser información general acerca de su computadora (tal como dirección IP, el dominio que usó para conectarse (e.g., .edu, .com, .net), y el tipo de navegador que usó). También podría ser información más específica acerca de sus hábitos de navegación (tal como la última vez que visitó un sitio web en particular o sus preferencias personales para mirar ese sitio).

Las cookies pueden quedar guardados durante extensiones de tiempo diferentes:

- **Cookies de sesión** – son las que almacenan información a medida que usted está usando el navegador; una vez que cierra el navegador, la información se borra. El fin primario de las cookies de sesión es ayudar con la navegación tal como indicar si usted ya visitó o no una página en particular y retener información acerca de sus preferencias una vez que visitó la página.
- **Cookies persistentes** – se almacenan en su computadora para que sus preferencias personales puedan ser retenidas. En la mayoría de los navegadores, puede ajustar la duración del tiempo para el almacenamiento de las cookies persistentes. Es debido a estas cookies que su dirección de correo electrónico aparece por default cuando abre su cuenta de correo electrónico Yahoo! o Hotmail, o su página de inicio personalizada cuando visita su comerciante online preferido. Si un atacante gana acceso a su computadora, puede recolectar su información personal a través de estos archivos.

Para incrementar su nivel de seguridad, considere ajustar sus valores de privacidad y seguridad para bloquear o limitar cookies en su navegador web.

Para asegurarse de que otros sitios no están recolectando información personal suya sin su conocimiento, **elija sólo permitir cookies para el sitio web que está visitando; bloquear o limitar las cookies de un tercero**. **Si está usando una computadora pública, debería asegurarse que los cookies están deshabilitados para prevenir que otra gente acceda o use su información personal.**

5. Consejo de Seguridad Informática ST05-010

Saber qué son los Certificados de Sitio Web

Usted pudo haber estado expuesto a un sitio web, o host, certificados si alguna vez clicqueó en el candado de su navegador o, cuando visita un sitio web, se le ha presentado un cuadro de diálogo aclamando que hay un error con el nombre o la fecha en el certificado. Comprender qué son estos certificados puede ayudarlo a proteger su privacidad.

¿Qué son certificados de sitio web?

Si una organización quiere tener un sitio web seguro que usa encriptado, necesita obtener un certificado de sitio, o host. Algunos pasos que puede tomar para que lo ayuden a determinar si un sitio usa encriptado es buscar un candado cerrado en la barra de estado al pie de la ventana de su navegador y buscar "https:" más que "http:" en el URL. Asegurándose que un sitio web encripta su información y que tiene un certificado válido, puede ayudarlo a protegerse contra los atacantes que crean sitios maliciosos para recolectar información. Usted quiere estar seguro de saber dónde está yendo su información antes de informar algo.

Si un sitio web tiene un certificado válido, significa que una autoridad que da el certificado ha tomado los pasos para verificar que la dirección web realmente pertenece a esa organización. Cuando usted tipea un URL o sigue un link hacia un sitio web seguro, su navegador verificará las siguientes características del certificado:

1. que la dirección del sitio web concuerde con la dirección que está en el certificado
2. que el certificado esté firmado por una autoridad certificante y que el navegador lo reconozca como una autoridad “de confianza”

¿Puede confiar en un certificado?

El nivel de confianza que usted pone en un certificado está relacionado con su grado de confianza con respecto a la organización y la autoridad certificante. Si la dirección web concuerda con la dirección del certificado, el certificado está firmado por una autoridad certificante confiable, y la fecha es válida, usted puede tener confianza de que el sitio que quiere visitar es realmente el sitio que está visitando. Sin embargo, a

menos que verifique personalmente la huella digital única de ese certificado llamando a la organización directamente, no hay forma de estar absolutamente seguro.

Cuando usted confía en un certificado, está esencialmente confiando en la autoridad certificante para que verifique la identidad de la organización para usted. Sin embargo, es importante saber que las autoridades certificantes varían en cuanto a lo estrictas que son acerca de la validación de toda la información en las solicitudes y en cuanto a asegurarle que sus datos son seguros. Por default, su navegador contiene una lista de más de 100 autoridades certificantes confiables. Esto significa que, por extensión, usted está confiando que todas esas autoridades certificantes verifican y validan la información adecuadamente. Antes de brindar cualquier información personal, tal vez quiera mirar el certificado.

¿Cómo verifica un certificado?

Hay dos formas de verificar el certificado del sitio web en Internet Explorer o Mozilla. Una opción es cliquear en el candado en la barra de estado de la ventana de su navegador. Sin embargo, su navegador puede no mostrar la barra de estado por default. También, los atacantes pueden crear sitios webs maliciosos con un ícono de candado falso y mostrar una ventana de diálogo falsa si cliquea sobre ese ícono. Una forma más segura de encontrar información acerca del certificado es buscar la función certificado en el menú de opciones. Esta información puede estar debajo de las propiedades del archivo o la opción de seguridad dentro de la página de información. Obtendrá un cuadro de diálogo con información acerca del certificado, incluyendo lo siguiente:

- **Quién emitió el certificado** – Debería asegurarse que el emisor es una autoridad certificante legítima y confiable (puede ver nombres tales como VeriSign, thawte, o Entrust). Algunas organizaciones también tienen sus propias autoridades certificantes que acostumbran a emitir certificados a sitios internos tales como las intranets.
- **A quién se le emitió el certificado** – El certificado debería ser emitido para la organización que posee el sitio web. No confíe en el certificado si el nombre en el certificado no concuerda con el nombre de la organización o persona que usted espera.
- **Fecha de expiración** – La mayoría de los certificados se emiten para uno o dos años. Una excepción es el certificado para la autoridad certificante misma, la cual, debido al grado de participación necesaria para distribuir la información para todas las organizaciones que mantienen sus certificados, puede ser de diez años. Esté atento a las organizaciones con certificados que son válidos durante más de dos años o con certificados que se vencieron.

Cuando visite un sitio web, tal vez se le presente un cuadro de diálogo con el certificado del sitio. Esto puede ocurrir si el nombre del certificado está registrado y no concuerda con el nombre del sitio, usted ha elegido no confiar en la empresa que emitió el certificado, o el certificado ha vencido. Generalmente se le presentará la opción de examinar el certificado, luego de lo cual usted puede aceptarlo para

siempre, o elegir no aceptarlo. La confusión a veces es fácil de resolver (tal vez el certificado fue emitido a un departamento en particular dentro de la organización más que el nombre en el archivo). Si no está seguro que el certificado es válido o cuestiona la seguridad del sitio, no brinde información personal. Aún si la información está encriptada, asegúrese de leer la política de privacidad de la organización primero para saber qué es lo que se está haciendo con esa información.

6. Consejo de Seguridad Informática ST05-016

Saber qué son los Nombres de Dominio Internacionalizados

Tal vez usted estuvo expuesto a nombres de dominio internacionalizados (IDNs) sin darse cuenta. Mientras que típicamente no afectan su actividad de navegación, los IDNs pueden dar a los atacantes una oportunidad para redirigirlo a una página web maliciosa.

¿Qué son los nombres de dominio internacionalizados?

Para disminuir la cantidad de confusión en torno a los diferentes idiomas, hay un estándar para los nombres de dominio dentro de los navegadores web. Los nombres de dominio están incluidos en el URL (o dirección web) del sitio web. Este estándar está basado en el alfabeto romano (usado por el idioma inglés), y las computadoras convierten varias letras en equivalentes numéricos. Este código se conoce como ASCII (American Standard Code for Información Interchange). Sin embargo, otros idiomas incluyen caracteres que no se traducen en este código, motivo por el cual se introdujeron los nombres de dominio internacionalizados.

Para compensar con los idiomas que incorporan caracteres especiales (tales como Español, Francés o Alemán) o confían completamente en la representación de caracteres (tal como los idiomas Asiáticos o Árabes), se tuvo que desarrollar un nuevo sistema. En este nuevo sistema, el URL base (que es generalmente la dirección para la página de inicio) es disectada y convertida en un formato que es compatible con ASCII. El URL resultante (que contiene el hilo "xn--" tanto como una combinación de letras y números) aparecerá en la barra de estado de su navegador. En nuevas versiones de muchos navegadores, también aparecerá en la barra de dirección.

¿Cuáles son algunas de las preocupaciones con respecto a seguridad?

Los atacantes pueden aprovechar los nombres de dominio internacionalizados para iniciar ataques phishing. Debido a que hay ciertos caracteres que pueden parecer ser iguales pero tienen códigos ASCII diferentes (por ejemplo la "a" Cyrillic y la "a" Latina), un atacante puede crear un URL de página web fraudulento (*"spoof"*). En lugar de ir a un sitio legítimo, puede ser dirigido a un sitio malicioso, que podría parecer idéntico al real. Si brinda información personal o financiera en el sitio malicioso, el atacante puede recolectar esa información y luego usarla y/o venderla.

¿Cómo puede protegerse?

- **Tipear un URL en lugar de seguir un link** – Tipear un URL en un navegador en lugar de cliquear un link dentro de una página web o mensaje de correo electrónico minimizará su riesgo. Haciendo esto, es muy probable que visite el sitio legítimo en lugar del sitio malicioso que sustituye caracteres que parecen iguales.
- **Mantener su navegador actualizado** – Las versiones más viejas de los navegadores facilitaron a los atacantes para falsear (*spoof*) URLs, pero la mayoría de los navegadores más nuevos incorporan ciertas protecciones. En lugar de mostrar el URL que usted "piensa" que está visitando, la mayoría de los navegadores ahora muestran el URL convertido con el hilo "xn--".
- **Verificar la barra de estado de su navegador** – Si usted lleva su mouse sobre un link en una página web, la barra de estado de su navegador generalmente mostrará el URL al que el link refiere. Si ve un URL que tiene un nombre de dominio no esperado (tal como uno con el hilo "xn--" mencionado arriba), probablemente haya encontrado un nombre de dominio internacionalizado. Si no estaba esperando un nombre de dominio internacionalizado o sabe que el sitio legítimo no necesitaría uno, tal vez reconsidere visitar el sitio. Los navegadores como el Firefox incluyen una opción en sus valores de seguridad acerca de permitir o no que el texto de la barra de estado sea modificado. Para prevenir que los atacantes tomen ventaja de JavaScript y que parezca que usted está en un sitio legítimo, podría querer asegurarse que esta opción no está habilitada.

7. Consejo de Seguridad Informática ST05-015

Saber qué es la Tecnología Bluetooth

Muchos dispositivos electrónicos ahora están incorporando la tecnología Bluetooth que permite una comunicación inalámbrica con otros dispositivos Bluetooth. Antes de usar un Bluetooth, es importante comprender qué es, qué riesgos de seguridad presenta, y cómo protegerse.

¿Qué es Bluetooth?

Bluetooth es una tecnología que permite que dispositivos se comuniquen entre sé sin cables. Es un “estándar” electrónico, que significa que los fabricantes que quieren incluir esta característica deben incorporar requerimientos específicos dentro de sus dispositivos electrónicos. Estas especificaciones aseguran que los dispositivos pueden reconocer e interactuar con otros dispositivos que usan la tecnología Bluetooth.

Muchos fabricantes populares están haciendo dispositivos que usan tecnología Bluetooth. Estos dispositivos incluyen teléfonos móviles, computadoras y asistentes digitales personales (personal digital assistants - PDAs). La tecnología Bluetooth se apoya sobre una frecuencia de radio de corto rango, y todo dispositivo que incorpora

la tecnología se puede comunicar siempre que esté dentro de la distancia requerida. La tecnología a menudo se utiliza para permitir que dos tipos diferentes de dispositivos se comuniquen entre sí. Por ejemplo, usted puede operar su computadora con teclado inalámbrico, usar un auricular inalámbrico para hablar por su teléfono móvil o agregar una cita al calendario del PDA de su amigo desde su propio PDA.

¿Cuáles son algunas preocupaciones en cuanto a la seguridad?

Dependiendo de cómo está configurada, la tecnología Bluetooth puede ser bastante segura. Puede aprovechar que utiliza autenticación de llave (Firma Digital) y encriptado. Lamentablemente muchos dispositivos Bluetooth se apoyan sobre números de PIN numéricos cortos en lugar de contraseñas o frases contraseña más seguras.

Si una persona "descubre" su dispositivo Bluetooth, puede enviarle mensajes no solicitados o hacer un mal uso de su servicio Bluetooth, que podría provocar que le cobren cargos extras. Lo que sería peor, un atacante puede encontrar una forma de acceder o corromper sus datos. Un ejemplo de este tipo de actividad es "bluesnarfing," que se refiere a los atacantes que usan una conexión Bluetooth para robar información de su dispositivo Bluetooth. También los virus u otro código malicioso pueden aprovechar la tecnología Bluetooth para infectar otros dispositivos. Si usted está infectado, sus datos pueden ser corrompidos, comprometidos, robados o perdidos. Debería estar alerta a los intentos de que lo convenzan de enviar información a alguien que no confía a través de una conexión.

¿Cómo puede protegerse?

- **Deshabilitar el Bluetooth cuando no lo esté usando** – A menos que esté transfiriendo información en forma activa desde un dispositivo a otro, deshabilite la tecnología para prevenir que personas no autorizadas accedan a él.
- **Usar el Bluetooth en modo "oculto"** – Cuando tiene el Bluetooth habilitado, asegúrese que esté en modo "oculto," no "encontrable." El modo oculto previene que otros dispositivos Bluetooth reconozcan su dispositivo. Esto no previene que use sus dispositivos Bluetooth juntos. Usted puede "poner en par" a los dispositivos para que ellos se puedan encontrar entre sí aún si están en modo oculto. Aunque los dispositivos (por ejemplo, un teléfono móvil y un auricular) necesitarán estar en el modo encontrable para que los dispositivos se ubiquen entre sí inicialmente, una vez que están "puestos en par" siempre se reconocerán sin necesidad de redescubrir la conexión.
- **Tener cuidado al usar Bluetooth** – Esté atento a su entorno cuando ponga los dispositivos en pares o los opere en modo encontrable. Por ejemplo, si usted está en un "hotspot," (*lugar que ofrece acceso Wi-Fi*) inalámbrico público, hay mayor riesgo de que alguien puede interceptar la conexión que si estuviera en su hogar o su auto.
- **Evaluar sus valores de seguridad** – La mayoría de los dispositivos ofrecen una variedad de valores y rasgos que usted puede configurar a medida para que

cumpla con sus necesidades y requerimientos. Sin embargo, habilitar ciertos valores puede dejarlo más vulnerable de ser atacado, por lo tanto deshabilite cualquier valor no necesario o conexiones Bluetooth. Examine sus valores, particularmente los de seguridad, y seleccione opciones que cumplen con sus necesidades sin incrementar el riesgo. Asegúrese que todas sus conexiones Bluetooth estén configuradas para requerir una conexión segura.

- **Aproveche las ventajas de las opciones de seguridad** – Busque qué opciones de seguridad ofrece su dispositivo Bluetooth, y aproveche las opciones como autenticación y encriptado.

8. Consejo de Seguridad Informática ST05-004

Evitar la Violación del Derecho de Autor

Aunque el derecho de autor pueda parecer un tema puramente legal, el uso de archivos no autorizados podría tener consecuencias de seguridad. Para evitar una acusación o proceso y minimizar los riesgos para su computadora, asegúrese que tiene permiso para usar cualquier información con derecho de autor, y sólo baje archivos autorizados.

¿Cómo se aplica la violación del derecho de autor para Internet?

La violación del derecho de autor se aplica cuando usted usa o distribuye información sin permiso de la persona u organización que tiene la propiedad de los derechos legales para la información. Incluir una imagen o caricatura en su sitio web o en un documento, bajar música ilegalmente, y piratear software son todas violaciones de derecho de autor. Mientras que estas actividades parecen inofensivas, podrían tener serias consecuencias legales y de seguridad.

¿Cómo saber si tiene permiso para usar algo?

Si encuentra algo en un sitio web que le gustaría usar (por ejemplo, un documento, un gráfico, una aplicación), busque información acerca de los permisos para usar, bajar, redistribuir o reproducir. La mayoría de los sitios web tienen una página de "términos de uso" que explican cómo puede usar la información de ese sitio. Generalmente puede encontrar un link a esta página en la información de contacto o política de privacidad del sitio, o al pie de la página que contiene la información que usted está interesado en usar.

Puede haber restricciones basadas en el propósito, método y audiencia. También puede tener que adherirse a condiciones específicas referidas a cuánta información tiene permitida usar o cómo se presenta y atribuye la información. Si no puede localizar los términos de uso, o si no parecen claros, contacte al individuo u organización que tiene el derecho de autor para pedir autorización.

¿Qué condiciones podría enfrentar?

- **Proceso/acusación**- Cuando se baja, reproduce o distribuye información ilegalmente, se corre el riesgo de una acción legal. Las penalidades varían desde advertencias y eliminación obligatoria de todas las referencias hasta multas costosas. Dependiendo de la severidad del delito, también puede haber encarcelación. Para compensar sus propios costos y el dinero que piensan que pierden por el software pirateado, los proveedores pueden incrementar los precios de sus productos.
- **Infección** – Los atacantes podrían tomar ventaja de sitios o redes que ofrecen bajadas no autorizadas (música, películas, software, etc.) incluyendo código dentro de los archivos que podrían infectar su computadora una vez que fueron instalados. Debido a que usted no sabría la fuente o identidad de la infección (o aún que tal vez estaba ahí), usted tal vez no podría identificarlo o removerlo. Generalmente en mensajes spam de correo electrónico se hace propaganda de software pirateado con Troyanos ocultos como software con descuento.

Referencias

- Oficina de Derecho de Autor de EEUU (U.S. Copyright Office) - <http://www.copyright.gov/>
- Derecho de Autor en Internet (Copyright on the Internet) - <http://www.fplc.edu/tfield/copynet.htm>