2021

CONCEPTOS DE SEGURIDAD A CONSIDERAR CUANDO USAMOS LA COMPUTADORA

Nuevas Tecnologías de la Información y la Comunicación

M.I.S.T. Miguel Ángel Romero Ochoa

Universidad de Sonora

1-1-2021

CONTENIDO

Miguel Ángel Romero Ochoa
Espacio educativo NTIC
Universidad de Sonora

CONCEPTOS DE SEGURIDAD A CONSIDERAR CUANDO USAMOS LA COMPUTADORA

La sensación de anonimato, la necesidad de relacionarse, el número de servicios accesibles para los jóvenes, entre otros, son factores a tener en cuenta y que requieren medidas de seguridad.

Evidentemente, el problema de la seguridad en los sistemas de datos e información ha sido una preocupación desde los orígenes de estos sistemas.

Aunque hoy en día es prácticamente imposible considerar a los equipos informáticos como entes aislados, si consideramos la computadora como un elemento individual hay sólo tres elementos sobre los que tendremos que incidir para evitar agujeros de seguridad:

- Evitar accesos locales al equipo por parte de personas no deseadas.
- Evitar la contaminación del equipo por parte de elementos peligrosos que puedan dañar o poner muy lento el funcionamiento del mismo, y que se aprovechan fundamentalmente de los sistemas de almacenamiento portátiles (llaves USB, tarjetas SD, discos duros portátiles) y/o de los sistemas de comunicación.
- Evitar agujeros de seguridad mediante el mantenimiento actualizado del equipo informático, su sistema operativo y los programas que utilicemos.

Miguel Ángel Romero Ochoa
Espacio educativo NTIC
Universidad de Sonora

SEGURIDAD EN INTERNET

La seguridad en Internet es un reto fundamental en estos tiempos. El acceso a la red de redes se ha generalizado y con ello se acrecientan los riesgos y las amenazas. Víctimas especialmente vulnerables son los jóvenes que acceden desde sus casas y escuelas.

RIESGOS DE LA NAVEGACIÓN POR INTERNET

Los riesgos a la seguridad en los sistemas informáticos conectados a Internet se pueden clasificar según el objeto del ataque:

Hackers y crackers: Los hackers y los crackers son los individuos que están detrás de los procesos de vulneración de la seguridad que estamos describiendo. Los hackers se dedican a la búsqueda de agujeros de seguridad con el fin de explotarlos para acceder a sistemas aparentemente seguros. A diferencia de los Crackers, que vulneran los sistemas para realizar acciones delictivas, los Hackers, al menos en su origen, buscan más bien el prestigio personal de ser capaces de encontrar la manera de entrar en sistemas altamente protegidos.

Adware: Un código maligno que muestra publicidad no solicitada en su computadora.

Malware: se deriva de Malicious softWare (software maligno) y es un término general que incluye cualquier tipo de código dañino: “troyanos”, “gusanos”, “spyware”, “adware”, etc. que infiltran una computadora sin aprobación del usuario de la computadora y que están diseñados para dañar la computadora, recopilar información o permitir que se pueda controlar su computadora y usarla en forma para enviar spam (correo no deseado), etc.

Phishing: el intento de alguna persona para hacerse pasar por un negocio a fin de engañar y obtener información personal.

Spam (correo no deseado): Correo electrónico no solicitado que intenta venderle algo. También se conoce como *junk mail*.

Spyware: Es un software espía que utiliza su conexión de Internet para recopilar información acerca de usted sin su conocimiento o consentimiento y la envía a quien escribió el programa spyware. Al igual que el adware, a menudo se instala cuando se descargan programas 'freeware' o 'shareware'. El spyware puede estar viendo su información bancaria, información personal, etc. La forma en que se puede notar si se cuenta con este tipo de infección es la siguiente:

1. Se abren ventanas emergentes en el navegador de Internet.
2. Podrás ver en el navegador barras de herramientas que no instalaste.
3. Tu navegador te dirige a sitios web que no indicaste.
4. La página de inicio se cambia a una que no indicaste.

Virus: un programa de cómputo que puede duplicarse y extenderse de una computadora a otra.

Troyano: Es un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo le brinda a un atacante acceso remoto al equipo infectado. Los troyanos pueden realizar diferentes tareas, pero, en la mayoría de los casos permiten una administración remota (desde fuera) de tu equipo a un usuario no autorizado.

Un troyano no es de por sí, un virus informático, aun cuando teóricamente pueda ser distribuido y funcionar como tal. La diferencia fundamental entre un troyano y un virus, consiste en su finalidad. Para que un programa sea un "troyano" sólo tiene que acceder y controlar la computadora sin ser advertido, normalmente bajo una apariencia oculta. Al contrario que un virus, que es un huésped destructivo, el troyano no necesariamente provoca daños porque no es su objetivo.

Gusano informático: son programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones del ordenador. El objetivo de este malware suele ser

colapsar los ordenadores y las redes informáticas, impidiendo así el trabajo a los usuarios. A diferencia de los virus, los gusanos no infectan archivos.

El principal objetivo de los gusanos es propagarse y afectar al mayor número de ordenadores posible. Para ello, crean copias de sí mismos en el ordenador afectado, que distribuyen posteriormente a través de diferentes medios, como el correo electrónico, programas P2P o de mensajería instantánea, entre otros.

Los gusanos suelen utilizar técnicas de ingeniería social para conseguir mayor efectividad. Para ello, los creadores de malware seleccionan un tema o un nombre atractivo con el que camuflar el archivo malicioso. Los temas más recurrentes son los relacionados con el sexo, famosos, temas morbosos, temas de actualidad o software pirata.

Además, el uso de esta técnica aumenta considerablemente en fechas señaladas como San Valentín, Navidades y Halloween, entre otras.

Ransomware: Es un tipo de malware que los criminales instalan en su PC sin su consentimiento. Ransomware les da a los criminales la capacidad de bloquear su equipo desde una ubicación remota. Luego presentará una ventana emergente con un aviso que dice que su ordenador está bloqueado y afirma que no podrá acceder al mismo a no ser que pague.

Botnets: Representan uno de los delitos cibernéticos más sofisticados y populares de hoy en día. Permiten a los hackers tomar el control de muchos equipos a la vez y convertirlos en equipos "zombis", que funcionan como parte de un poderoso "botnet" que propaga virus, genera spam y comente otros tipos de delitos y fraudes. Un "bot" es un tipo de programa malicioso que permite a un atacante tomar el control de un equipo infectado. Por lo general, los bots, también conocidos como "robots web" son parte de una red de máquinas infectadas, conocidas como “botnet”, que comúnmente está compuesta por máquinas víctimas de todo el mundo.

Debido a que un equipo infectado por bots cumple las órdenes de su amo, muchas personas se refieren a estos equipos víctima como “zombis”.Los delincuentes cibernéticos que controlan estos bots son cada vez más numerosos.

Algunos botnets pueden englobar cientos o un par de miles de equipos, pero otros cuentan con decenas e incluso centenares de miles de zombis a su servicio. Muchos de estos equipos se infectan sin que sus dueños se enteren. ¿Existe algún indicio? Un bot puede hacer que su equipo funcione más lento, muestre mensajes misteriosos e, incluso, falle.

Rootkits: Es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers que consiguen acceder ilícitamente a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos. Hay rootkits para una amplia variedad de sistemas operativos, como Linux, Solaris o Microsoft Windows.

Tratan de encubrir a otros procesos que están llevando a cabo acciones maliciosas en el sistema. Por ejemplo, si en el sistema hay una puerta trasera para llevar a cabo tareas de espionaje, el rootkit ocultará los puertos abiertos que delaten la comunicación; o si hay un sistema para enviar spam, ocultará la actividad del sistema de correo. Al estar diseñados para pasar desapercibidos, no pueden ser detectados. Si un usuario intenta analizar el sistema para ver qué procesos están ejecutándose, el rootkit mostrará información falsa, mostrando todos los procesos excepto él mismo y los que está ocultando.

Keylogger: Es un tipo de software o dispositivo hardware que se encarga de registrar las pulsaciones que se realizan en el teclado y posteriormente “memorizarlos” y enviarlos a través de Internet, esto sin el consentimiento del usuario.

Miguel Ángel Romero Ochoa
Espacio educativo NTIC
Universidad de Sonora

SISTEMAS DE PROTECCIÓN

SISTEMAS DE PROTECCIÓN LOCAL

Desde el punto de vista de la protección de nuestra computadora, hay tres aspectos básicos a tener en cuenta, fáciles de implementar y que mejorarán sustancialmente nuestra experiencia de seguridad:

1.- Mantener actualizado el sistema operativo y el software instalado

Es fundamental, para evitar posibles agujeros de seguridad en los sistemas derivados de las vulnerabilidades explicadas anteriormente, que mantengamos permanentemente actualizado nuestro sistema y el software instalado. Para ello, en la actualidad, los sistemas de actualización automática de los sistemas operativos nos facilitan enormemente la labor, al detectar de manera autónoma la configuración de nuestros sistemas y la necesidad de actualización, al igual que ocurre con la mayoría de los programas instalados.

2.- Cambiar periódicamente la contraseña de acceso al sistema

Sea por el método que sea, si un usuario consigue las claves de acceso a un sistema, tendrá vía libre para operar con él sin nuestro consentimiento.

Para minimizar los riesgos derivados se debe cambiar con frecuencia la clave de acceso al sistema, utilizando para su configuración al menos una longitud de 6 caracteres alfanuméricos en los que combinar mayúsculas y minúsculas, letras, números y símbolos del tipo %, & o $.

Evidentemente hay que evitar palabras con significado común y relacionado con nuestro entorno próximo y no dejarlas al alcance de cualquiera en las proximidades de la computadora.

Existen muchas formas de crear contraseñas largas y complejas. Aquí le presentamos algunas sugerencias que podrían ayudarlo a recordar su contraseña de forma sencilla:

Qué hacer	**Ejemplo**
Comience con una frase o dos.	Debo colocar una contraseña compleja
Elimine los espacios entre las palabras de la frase.	Debocolocarunacontraseñacompleja
Abrevie palabras o escriba mal una de ellas intencionadamente.	DvocolocContraComp
Agregue números para que la contraseña sea más larga. Coloque números y símbolos que signifiquen algo para usted al final de la frase.	DvocolocContraComp1508$90%

Después de haber realizado lo anterior, pruebe la seguridad de su contraseña mediante un comprobador de seguridad de contraseñas.

Evita poner contraseñas con la siguiente estructura:

- Secuencias o caracteres repetidos, ejemplo: 123456, abcde, entre otros.
- Información personal: tu nombre, fecha de nacimiento, tus iniciales, entre otros.

Como hoy en día es habitual tener múltiples usuarios y contraseñas para acceso no sólo al equipo local sino a múltiples sitios Web, existen programas que nos ayudan a recordarlas, algunos ejemplos de ellos son Password Genie, Splash Id, Roboform´s, KeePass, Norton Password Manager, entre otros.

3.- Instalar y mantener actualizado un programa antivirus

Los programas antivirus monitorizan de manera permanente el sistema en busca de software malicioso en ejecución o en estado latente, con el fin de identificarlo, dar la alarma y si fuera posible desinfectar el equipo o al menos aislar el virus. Existen múltiples sistemas antivirus de diferentes empresas y algunas soluciones gratuitas aunque es difícil establecer cuál de todas ellas es la mejor puesto que las comparativas realizadas por revistas especializadas usan unos parámetros muy diversos de evaluación y no exentos de influencias de las compañías explotadoras de las soluciones.

4.- Instalar y mantener actualizado un programa antispyware

El Antispyware es un tipo de software diseñado para detectar y eliminar programas maliciosos o amenazantes en un ordenador. Estos programas se llaman spyware como alusión a su tendencia a obtener y enviar información personal de un individuo a un tercero sin su consentimiento. Los Antispyware están disponibles en varios formatos, y en muchos precios diferentes.

Los mejores antispyware se encuentran en los programas antivirus profesionales. Estos programas combinan la seguridad en Internet, un antivirus y un antispyware en un solo producto.

SISTEMAS DE PROTECCIÓN PERIMETRAL Y NAVEGACIÓN SEGURA

La instalación de un firewall es otra medida eficaz que se puede tomar para proteger su computadora de amenazas. Un firewall permite filtrar el tráfico de Internet antes de que llegue a una computadora o una red privada. Ofrece asimismo protección adicional contra amenazas, como piratas informáticos y virus. Un firewall ayuda

además a garantizar la privacidad de la computadora, ya que restringe el acceso externo a la computadora por parte de algún usuario no autorizado.

Los Firewall se basan en listas de control de acceso en las que se definen direcciones y/o programas a los que se permite el acceso a Internet (listas blancas) o se les deniega el acceso (listas negras).

SISTEMAS DE CONTROL PARENTAL

Basados en los sistemas de filtrado mencionados anteriormente, éstos son sistemas diseñados para garantizar una experiencia segura de navegación por parte de los niños y los jóvenes. Los mismos navegadores de Internet (Internet Explorer, Firefox, Safari, etc.) disponen de su propio sistema de control parental.

Los filtros de control verifican todos los paquetes de información que atraviesan por la red, capturándolos, analizándolos conforme a patrones de seguridad establecidos y bloqueándolos en el caso de que se encuentre que contienen información no deseada, según las definiciones que hayan marcado los administradores o responsables de los sistemas.

CONSEJOS PARA MINIMIZAR LOS RIESGOS EN LA NAVEGACIÓN POR INTERNET

CONSEJOS PARA UNA NAVEGACIÓN SEGURA

1. Para evitar virus, descarga los ficheros solo de fuentes confiables.

2. Descarga los programas desde las páginas oficiales para evitar suplantaciones.
3. Analiza con un antivirus todo lo que descargues antes de ejecutarlo.
4. Mantén actualizado el navegador y sistema operativo para protegerlo contra los últimos ataques.
5. Como apoyo para saber si una página es confiable utiliza analizadores de URLs.
6. Elimina de tu navegador el historial de búsquedas, cookies y archivos temporales de Internet.
7. Ten precaución con las contraseñas que guardas en el navegador.
8. Redes sociales, correo electrónico y portales bancarios, permiten la autenticación en dos pasos, lo cual, es una recomendación a seguir para proteger el acceso no autorizado.

CONSEJOS PARA EL USO SEGURO DEL CORREO ELECTRÓNICO

1. Desconfía de los correos de remitentes desconocidos, ante la duda elimínalo.
2. No abras ficheros adjuntos sospechosos procedentes de desconocidos o que no hayas solicitado.
3. Utiliza el filtro anti-spam y marca los correos no deseados como correo basura.
4. Ten precaución con el mecanismo de recuperar contraseña, utiliza una pregunta que sólo tu sepas responder.
5. Analiza los adjuntos con un antivirus antes de ejecutarlos en tu sistema.
6. Desactiva la vista previa y la visualización en HTML de tu cliente de correo para evitar el posible código malicioso que pueda estar incluido en el cuerpo de los mensajes.
7. No facilites tu cuenta de correo a desconocidos.

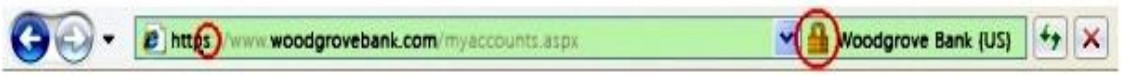
8. No respondas a mensajes falsos, ni a cadenas de correos para evitar que tu dirección se difunda.

9. Cuando reenvíes mensajes a múltiples destinatarios utiliza la copia carbón oculta –CCO o BCC- para introducir las direcciones.

CONSEJOS PARA COMPRAR EN LÍNEA DE FORMA SEGURA

1. Use sitios Web que conozca: Empiece en un sitio seguro en vez de comprar mediante un motor de búsqueda.

2. Busque el Candado: Nunca jamás compre algo por Internet con su tarjeta de crédito en un sitio que no tenga instalado el cifrado SSL (secure sockets layer, nivel de seguridad en las conexiones) cuando menos. Puede saber cuándo un sitio tiene SSL porque el URL de dicho sitio empezará con HTTPS:// (en vez de solo HTTP://). Aparecerá un icono con un candado cerrado, generalmente en la barra de estado en la parte inferior de su navegador de Internet o justo a un lado del URL en la barra de dirección.



3. Busque los sellos de aprobación de terceros: Las compañías solo pueden exhibir estos sellos en sus sitios si se ajustan a un grupo de estándares rigurosos sobre, por ejemplo, el modo en que se puede usar la información personal. Se deben buscar dos sellos.

Better Business Bureau Online—(BBBOnline)

o

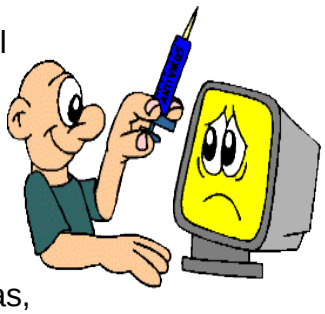
TRUSTe

Si encuentras los sellos, haz click sobre ellos para asegurarte que te lleven a las organizaciones que los han creado. Algunos vendedores sin escrúpulos exhiben esos logotipos en su sitio sin permiso.

4. No diga todo: Ninguna tienda para compras por Internet necesita su número de seguro social ni su cumpleaños para poder hacer negocios. Cuando sea posible, proporcione la menor cantidad de información.

5. Verifique sus estados de cuenta: Entre a Internet con regularidad y busque los estados de cuenta de su tarjeta de crédito, tarjeta de débito y cuentas de cheques. Si ve algo mal, tome el teléfono para atender rápidamente el asunto.

6. Vacune su PC: Necesita estar protegido en contra del malware con actualizaciones regulares de su programa de antivirus.



7. Use contraseñas seguras: Queremos recalcar insistentemente que se asegure de usar contraseñas seguras, pero con mucha mayor importancia cuando se trate de bancos o compras en línea.

8. Use comunicaciones móviles: No hay necesidad de preocuparse más al hacer compras con un dispositivo móvil que por Internet. El truco es usar las aplicaciones provistas directamente por las tiendas, como Amazon, Target, etc.

9. Evite las terminales y redes públicas: Es de esperar que no tenemos que decirle que es una mala idea usar una computadora pública para efectuar compras, pero sí lo haremos. Si lo hace, solo recuerde cerrar su sesión cada vez que use una terminal pública, incluso si solo revisó su correo electrónico.

10. Haga privada su conexión inalámbrica (Wi-Fi): Si decide hacer compras con su computadora móvil, necesitará una conexión inalámbrica. Solo use la conexión inalámbrica si tiene acceso a Internet a través de una conexión de red virtual privada (VPN, virtual private network).

11. Cuidado con las tarjetas de regalo: Las tarjetas de regalo son el regalo para las fiestas más solicitado, y este año no será la excepción. Hágalo con el proveedor cuando compre una; a los estafadores les gusta subastar tarjetas de regalo sin fondos o con muy pocos fondos en sitios como eBay.

12. Conozca lo que es demasiado bueno para ser cierto: En la mayoría de los casos, el escepticismo le puede ahorrar el robo de un número de tarjeta.

SUGERENCIAS DE SEGURIDAD EN LAS REDES SOCIALES

Los sitios Web de redes sociales como Facebook, Instagram y Twitter son servicios que pueden usar las personas para conectarse con otros y compartir información como fotografías, videos y mensajes personales. A medida que crece la popularidad de estos sitios, también crecen los riesgos de su uso.

1. Tenga precaución cuando haga clic en vínculos que reciba en mensajes de sus amigos en su sitio Web social. Trate a los vínculos en los mensajes de estos sitios como lo haría con los vínculos en mensajes de correo electrónico.

2. Sepa lo que ha publicado acerca de usted mismo. Una forma común que utilizan los hackers para tener acceso a sus cuentas financieras o de otro tipo es hacer clic en el vínculo "Forgot your password? (¿Olvidó su contraseña?)" en la página de inicio de sesión de la cuenta. Para entrar sin autorización a su cuenta, buscan las respuestas de sus preguntas de seguridad, como cumpleaños, ciudad natal, generación de preparatoria o apellido materno.

3. No confíe en que un mensaje proviene realmente de quien dice. Los hackers pueden entrar sin autorización a las cuentas y enviar mensajes que parecen que son de sus amigos, pero que no lo son. Si sospecha que un mensaje es fraudulento, use un método alterno para contactar a su amigo e investigarlo.

4. Para evitar dar direcciones de correo electrónico a sus amigos, no permita que los servicios de redes sociales revisen su libreta de direcciones de correo electrónico. Cuando se una a una nueva red social, es posible que reciba una oferta de introducir su dirección de correo electrónico y su contraseña para saber si sus contactos están en la red. El sitio puede usar esta información para enviar mensajes condicha dirección de correo electrónico a todas las personas en su lista de contactos o incluso a alguien a quien en alguna ocasión haya enviado un

mensaje de correo electrónico. Los sitios de redes sociales deben explicar lo que harán con ello, pero algunos no lo hacen.

5. Escriba directamente en su navegador la dirección de su sitio de red social o use sus marcadores personales. Si hace clic en un vínculo a su sitio a través de correos electrónicos u otro sitio Web, es posible que introduzca su nombre de cuenta y su contraseña en un sitio falso donde pueden robar su información personal.

6. Sea selectivo con las personas que acepte como amigos en una red social. Los usurpadores de identidades pueden crear perfiles falsos para obtener información por parte de usted.

7. Elija cuidadosamente su red social. Evalúe el sitio que planee utilizar y asegúrese de comprender la política de privacidad. Investigue si el sitio monitorea el contenido que publican las personas. Usted proporcionará información personal a este sitio Web, así que use los mismos criterios que usaría para seleccionar un sitio donde introduzca su tarjeta de crédito.

8. Asuma que todo lo que coloca en un sitio de red social es permanente. Incluso si puede borrar su cuenta, cualquier persona en Internet puede imprimir fácilmente fotografías o texto o guardar imágenes y videos a una computadora.

9. Tenga cuidado al instalar funciones adicionales en su sitio. Muchos sitios de redes sociales le permiten descargan aplicaciones de terceros que le permiten hacer más con su página personal. Para descargar y usar aplicaciones de terceros con seguridad, tome las mismas precauciones de seguridad que tomaría con cualquier otro programa o archivo que descargue de Internet.

REFERENCIAS

- Aspectos básicos del Internet y seguridad cibernética. Technology expertise, Access & learning for all texans. Recuperado de:

  https://www.tsl.texas.gov/sites/default/files/public/tslac/u34/Internet%20y%20Seguridad%20Cibern%C3%A9tica.pdf

- Seguridad en Internet. Recursos Tic. Recuperado de:

  http://recursostic.educacion.es/observatorio/web/es/component/content/article/805-monografico-seguridad-en-internet

- Cree contraseñas seguras. Microsoft. Recuperado de:

  http://www.microsoft.com/es-xl/security/online-privacy/passwords-create.aspx

- Cómo comprar en línea de forma más segura. Microsoft. Recuperado de:

  http://www.microsoft.com/es-xl/security/online-privacy/online-shopping.aspx

- ¿Que es el Ransomware?. Microsoft. Recuperado de:

  https://www.microsoft.com/es-es/security/resources/ransomware-whatis.aspx

- Bots y botnets: Una amenaza creciente. Norton by Symantec. Recuperado de:

  http://mx.norton.com/botnet

- Gusanos informáticos. Panda. Recuperado de:

  http://www.pandasecurity.com/mexico/homeusers/security-info/classic-malware/worm/

- ¿Qué son los Rootkits? InfoSpyware. Recuperado de:

  https://www.infospyware.com/articulos/que-son-los-rootkits/

- ¿Qué es Antispyware? Valor Top. Recuperado de:

  http://www.valortop.com/blog/que-es-el-antispyware