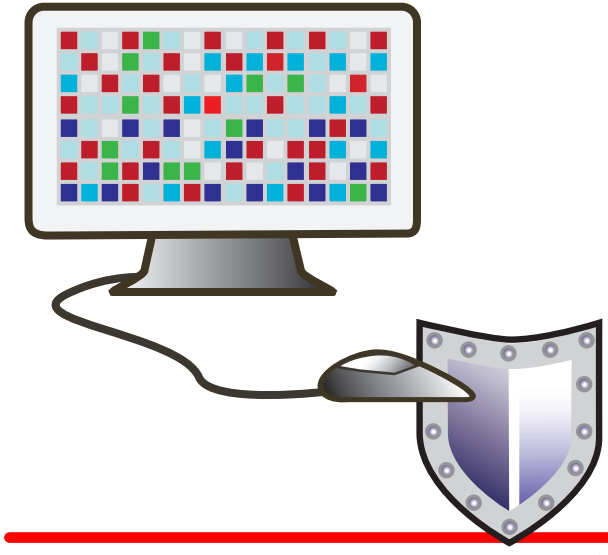
LA SEGURIDAD INFORMÁTICA:
una responsabilidad de todos

Las computadoras y el Internet son blancos populares para los delincuentes. Sin protección, los ladrones pueden invadir su computadora y robar números de tarjetas de crédito, información de cuentas bancarias y otros datos personales sensibles.

Todos los usuarios de computadoras deben tomar medidas para aumentar la seguridad y reducir las posibilidades de daños a su persona y su computadora. Aquí le presentamos algunos consejos comunes de seguridad informática para saber cómo mantener su computadora segura.



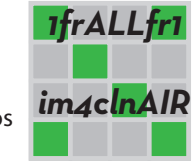
Virus y gusanos

Un "virus" informático se adhiere a los programas que se encuentran en su computadora y daña los programas, la información o el equipo. Un "gusano" informático ocasiona lo mismo y además se duplica a si mismo. Estos pueden dañar su computadora e infectar otras también.

MEDIDAS:

A continuación le presentamos cosas que puede hacer ahora mismo que no le tomarán mucho tiempo ni le costarán mucho dinero. Algunas de ellas sólo requieren un cambio de hábito.

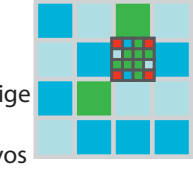
Contraseñas



Las contraseñas protegen los datos que usted guarda en su computadora, incluyendo cuentas privadas, documentos y el acceso a información identificatoria.

La mejor manera de evitar que los invasores cibernéticos ("hackers") y otras personas descifren su contraseña es intentar usar una combinación de letras, números y caracteres (por ejemplo, !, @, #, $, %). Y más importante aún, nunca comparta su contraseña con nadie. Mantenga un registro de las contraseñas en un sitio seguro y cámbielas con regularidad.

Parches y actualizaciones



Un parche o una actualización es un pequeño programa informático que corrige los problemas de programas conocidos. Las empresas de informática lanzan nuevos parches con frecuencia y le notifican de actualizaciones que son necesarias a través del Internet o por correo electrónico si usted ha registrado el producto.

Es importante que continúe instalando los parches más recientes. Puede configurar su computadora para que lo haga de manera automática. La computadora verificará con las empresas de informática para corregir sus sistemas operativos, navegador de Internet y sus programas antivirus.

Firewalls y programas de protección contra virus y programas de espionaje

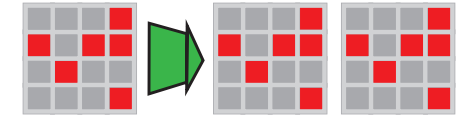
Los firewalls son sistemas que actúan como filtro al restringir el movimiento de la información entre los sistemas informáticos conectados en red. Ellos evitan que se filtre información privada y se instalen programas no deseados.

Los programas de protección contra virus, o programas antivirus, intentan identificar, neutralizar o eliminar los programas maliciosos. Estos programas intentan ya sea "limpiar" o "desinfectar" el virus, ponerlo en "cuarentena" o "destruirlo" al realizar un escaneo de su computadora con regularidad.

A través de las configuraciones de su navegador de Internet, usted puede aumentar las configuraciones de seguridad y bloquear las publicidades emergentes.

Se encuentran a disposición firewalls y programas antivirus gratuitos y fáciles de utilizar. Encuentre información en línea acerca de estos programas bajo la búsqueda de "programas de firewalls" o "programas antivirus".

Hacer copias



Hacer copias de archivos o documentos importantes de su computadora es tan importante como hacer copias adicionales de su partida de nacimiento o pasaporte. Puede proteger sus documentos y archivos grabándolos en un disco, dispositivo de almacenamiento USB, almacenamiento en Internet u otros equipos de almacenamiento. Hágalo regularmente.

LISTA DE VERIFICACIÓN

A continuación le presentamos una lista de verificación de medidas que los usuarios particulares pueden adoptar para proteger sus computadoras. Esta lista ha sido elaborada por el Centro de Coordinación del Equipo de Respuesta para Emergencias Informáticas (CERT, por sus siglas en inglés). Puede obtener más detalles en :www.cert.org/tech_tips/home_networks.html.

- Utilice programas de protección contra virus
- Utilice un firewall.
- No abra adjuntos de mensajes de correo de personas desconocidas.
- No instale programas cuyo origen desconoce.
- Deshabilite las extensiones de los nombres de archivos ocultos.
- Mantenga todas las aplicaciones (incluso el sistema operativo) actualizados.
- Apague su computadora o desconéctese del Internet cuando no esté en uso.

Espías y publicidades no deseadas

Todos desean proteger su privacidad. Desafortunadamente, los programas de espionaje ("spyware") y los programas de publicidad ("adware") pueden instalarse en su computadora sin su permiso.

Usted puede instalar estos programas en su computadora sin darse cuenta al visitar ciertos sitios de Internet, hacer clic en los enlaces, bajar archivos del Internet o abrir adjuntos en los mensajes de correo.

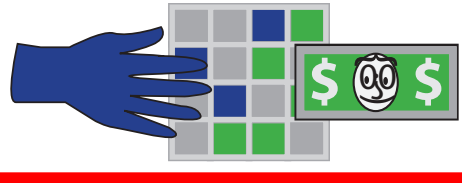
Los programas de espionaje recopilan datos personales y los envían a los delincuentes. Los programas de publicidad muestran material publicitario no deseado en ventanas emergentes o crean una barra de publicidad en la pantalla de su computadora.

Mensajes de correo desagradables y esquemas para robarle su dinero

No responda los mensajes de correo basura, ¡bórrelos! Únicamente abra los mensajes de correo o haga clic en los enlaces que provienen de personas que conoce y en quienes confía.

El "correo no solicitado" (conocido como spam en inglés) es el mensaje de correo basura que usted nunca solicitó. No responda a los mensajes, simplemente bórrelos.

El "fraude electrónico" (phishing, en inglés) es una estafa en línea que utiliza mensajes de correo electrónico no solicitados o mensajes emergentes para inducirle a que comparta información personal, su número de Seguro Social o contraseñas. Las "personas que cometen fraude electrónico" (phishers, en inglés) disfrazan sus mensajes de correo electrónico y sitios de Internet como bancos u otras instituciones confiables. Ellos intentan engañarle para que proporcione sus números de cuentas y contraseñas. No responda ni haga clic en los enlaces donde se le solicita información personal. ¡Bórrelos!



Asimismo, visite el sitio de Internet de Seguridad Informática de Seattle en: www.seattle.gov/informationsecurity.

Además, puede visitar el Sitio de Seguridad de Microsoft para obtener información en varios idiomas. Visítelos en: http://www.microsoft.com/protect y seleccione su idioma haciendo clic en "worldwide sites" (sitios a nivel mundial).

OBTENER AYUDA

Puede solicitar copias impresas de esta información llamando al (206) 233-7877 o escribiéndonos a PO Box 94709, Seattle, WA, 98124-4709.

Las bibliotecas públicas locales y los centros tecnológicos comunitarios son también importantes fuentes para obtener mayor información. Consulte: www.seattle.gov/tech/techmap

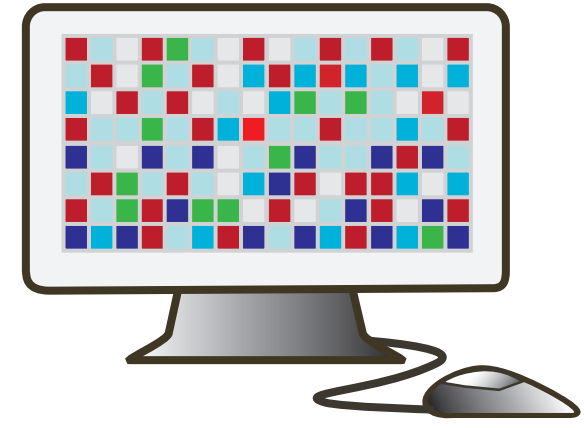
También puede obtener ayuda de las empresas de apoyo técnico y foros en línea. Los informes de consumidores, las revistas de informática, los fabricantes y vendedores de computadoras y las empresas de software también pueden proporcionarle información útil.

Este folleto ha sido elaborado por el Programa de Tecnología de la Comunidad y la Oficina de Seguridad Informática del Departamento de Tecnología de la Información de la Ciudad de Seattle.
www.seattle.gov/tech
www.seattle.gov/informationsecurity

Version 01/2010

City of Seattle
Department of Information Technology

¿ESTÁ SEGURA SU COMPUTADORA?



Sugerencias para proteger su computadora y su seguridad

City of Seattle
Department of Information Technology