Para. Piensa. Conectate.™ es la educación nacional de ciberseguridad y la campaña de sensibilización.

Consejos y recomendaciones

Consejo: mantenga limpia su computadora.

Recomendación:

- **Mantenga actualizado el software de seguridad:** tener actualizados el software de seguridad, el navegador web y el sistema operativo son las mejores defensas contra virus, software malicioso y otras amenazas en línea.
- **Automatice las actualizaciones de software:** muchos programas de software se conectarán y actualizarán de forma automática para defenderse contra riesgos conocidos. Active las actualizaciones automáticas si esta es una opción disponible.
- **Proteja todos los dispositivos que se conectan a Internet:** además de las computadoras, los teléfonos inteligentes, los sistemas de juegos y otros dispositivos web también necesitan protección contra virus y software malicioso.
- **Conecte y analice:** los dispositivos USB y otros dispositivos externos se pueden infectar con virus y software malicioso. Use su software de seguridad para analizarlos.

Consejo: proteja su información personal.

Recomendación:

- **Proteja sus cuentas:** pida protección adicional de las contraseñas. Muchos proveedores de cuentas ofrecen actualmente formas extras de verificar su identidad antes de realizar negocios en ese sitio.
- **Cree contraseñas largas y seguras:** combine letras en mayúscula y minúscula con números y símbolos para crear una contraseña más segura.
- **Cuenta única, contraseña única:** las contraseñas separadas para cada cuenta ayudan a frustrar los ataques informáticos.
- **Escríbala y protéjala:** todos podemos olvidar una contraseña. Mantenga una lista en un lugar seguro alejado de su computadora.
- **Controle su presencia en línea:** cuando sea posible, configure los parámetros de privacidad y seguridad en los sitios web al nivel de confianza deseado cuando comparta información. Es correcto limitar con quién comparte su información.

Consejo: conéctese con cuidado

Recomendación:

- **Ante la duda, es mejor eliminar:** los enlaces en los correos electrónicos, tweets, publicaciones y anuncios en línea son, a menudo, la forma que utilizan los atacantes cibernéticos para poner en riesgo su computadora. Si es sospechoso, aun si conoce de donde proviene, es mejor eliminarlo o, si corresponde, marcarlo como correo electrónico no deseado.
- **Conozca las zonas de cobertura Wi-Fi:** limite el tipo de transacciones que realiza y ajuste los parámetros de seguridad en su dispositivo para limitar quién tiene acceso a su computadora.
- **Proteja su dinero:** si realiza compras o transacciones bancarias, compruebe que el sitio tenga activada la seguridad. Busque direcciones web con "https://" o "shttp://", lo que significa que el sitio toma medidas adicionales para mantener la seguridad de su información. "Http://" no es seguro.

Consejo: manténgase informado sobre la web.

Recomendación:

- **Manténgase actualizado. Esté al tanto de las formas nuevas de mantenerse protegido en línea.** Visite los sitios web confiables para obtener la información más reciente y compartirla con amigos, familiares y colegas, y recomendarles que conozcan el funcionamiento de la web.
- **Piense antes de actuar:** desconfíe de las comunicaciones que le piden que actúe de inmediato, que ofrecen algo demasiado bueno para ser verdad o que piden información personal.
- **Haga copias de respaldo:** proteja su trabajo, música, fotos y demás información digital valiosa mediante una copia electrónica y guárdela en un lugar seguro.

Consejo: sea un buen ciudadano virtual.

Recomendación:

- **Seguro para mí, seguro para todos:** lo que hace en línea puede afectar a todos en el hogar, en el trabajo o alrededor del mundo. La práctica de buenos hábitos en línea favorece a toda la comunidad digital.
- **Publique información sobre otros de la misma manera que ellos publican sobre usted.**
- **Ayude a las autoridades a luchar contra el delito informático:** informe sobre identidades o finanzas robadas u otros delitos informáticos a http://www.ic3.gov/ (Centro de reclamaciones sobre delitos en Internet, Internet Crime Complaint Center), la Comisión Federal de Comercio (Federal Trade Commission) en http://www.ftc.gov/complaint (si se trata de un fraude), y a la autoridad competente o fiscalía local, según corresponda.

Para. Piensa. Conectate.™ Ponga en práctica estos consejos y anime a otros a que lo hagan.

Para obtener más información, visite www.stopthinkconnect.org/espanol.