La seguridad y protección en línea comienzan con usted

Todos los días, miles de millones de personas alrededor del mundo usan la Internet para trabajar, comprar, jugar, informarse y comunicarse con familiares y amigos. Para los niños, la Internet es un salón de clases y área de juegos virtuales a la vez. Para los adultos, es una herramienta poderosa.

Pero usar la Internet puede exponerlos a usted y a su familia a molestias como correo spam y mensajes instantáneos o a riesgos como robo de identidad, pedófilos y amenazas a su seguridad que pueden dañar su computadora o destruir su valiosa información.

Afortunadamente, usted puede tomar algunas medidas simples para ayudar a proteger su computadora, su familia y su información personal en línea. La información aquí proporcionada es un buen inicio. Para más consejos sobre seguridad en línea, visite www.microsoft.com/latam/protect.

Proteja su computadora

Con solo cuatro pasos básicos, usted puede ayudar a mantener su computadora a salvo de muchos ataques de software malicioso:

- Use un firewall y manténgalo activado — Los firewalls ayudan a proteger a su computadora, colocando una barrera protectora entre su computadora y la Internet, camuflándola ante los delincuentes y software malicioso como virus y gusanos.
- Mantenga su sistema operativo y su software actualizados — Una de las cosas más importantes que puede hacer para proteger su computadora es también una de las más fáciles: mantener su sistema operativo actualizado con el más reciente software, preferentemente utilizando un servicio que ofrezca actualización automática. Visite los sitios de Internet de los fabricantes de software para información sobre actualizaciones.
- Instale software antivirus y manténgalo actualizado — El software antivirus inspecciona todo lo que entra a su computadora—incluyendo correos electrónicos, discos y archivos de datos—buscando miles de virus conocidos y trabajando para eliminar a los que sean hallados. Suscríbase a un servicio de actualización de antivirus y descargue actualizaciones automáticamente para ayudar a proteger su computadora de las amenazas más recientes.
- Use software antiespía actualizado — El software antiespía revisa su computadora en busca de software espía y otro software potencialmente no deseado que rastrea su actividad en línea o hace cambios en su computadora. El software antiespía lo alerta sobre el software que detecta y le ayuda a tomar decisiones sobre cómo manejarlo. Al igual que con el software antivirus, actualice su software antiespía regularmente.

Proteja a su familia

Comprendiendo los beneficios y los riesgos del uso de Internet, y siguiendo unas pautas básicas, su familia podrá disfrutar de una experiencia en línea más segura:

- Hable con sus hijos acerca de lo que ellos hacen en línea — Explique a sus hijos los riesgos de la Internet y cómo su comportamiento puede incrementar o disminuir esos riesgos. Familiarícese con los juegos que sus hijos juegan en línea, con las salas de chat que visitan y con lo que escriben en sus blogs y en sus perfiles en sitios de redes sociales. Enseñe a sus hijos a confiar en sus instintos y a decirle inmediatamente si alguna vez se sienten amenazados o asustados por algo que sucede en línea.
- Establezca reglas claras para el uso de Internet — Establezca reglas claras acerca de cuándo y cómo sus hijos pueden usar la Internet y ponga las reglas cerca de la computadora. Deje claro que sus hijos no perderán su computadora u otros privilegios si le informan acerca de situaciones en línea que los hagan sentirse incómodos.
- No comparta su información personal — Enseñe a sus hijos a consultar con usted antes de compartir información personal sobre ellos o su familia. Enséñeles a ser muy cuidadosos al conversar con cualquier persona que no conozcan o que no sea de su confianza en el mundo real.
- Use software de seguridad familiar — Muchas compañías ofrecen tecnología de seguridad familiar para ayudarlo a administrar el uso de Internet de sus hijos. No existe una solución absoluta tecnológica que se acomode a las necesidades de todas las familias, así que asegúrese de revisar la lista completa de instrumentos populares para familias en www.navegaprotegido.org.

Proteja su información personal

Usted puede aprender a disminuir los riesgos comprendiendo de qué manera los delincuentes usan la Internet para cometer crímenes:

- Actúe inteligentemente cuando esté en línea — Ignore y borre el correo spam—cualquier oferta que parezca demasiado buena para ser cierta, probablemente lo sea. No divulgue su información financiera personal—no responda a correos electrónicos de su banco o institución financiera que soliciten información sobre su cuenta. En lugar de hacerlo, póngase en contacto directo con el banco vía telefónica o visitando directamente el sitio de Internet de su banco. Use contraseñas difíciles para aumentar su seguridad—al menos ocho caracteres que combinen letras, números y símbolos. No descargue archivos ni haga clic en links o documentos adjuntos a menos que sepa que puede confiar en la fuente de la cual provienen.
- Proteja su información personal — Antes de compartir información personal en un sitio de Internet, lea la declaración de privacidad. Verifique que la dirección de Internet contenga **https** u otra señal de que el sitio protege la información confidencial. Compare el nombre de la dirección de Internet con el certificado de seguridad para asegurarse de que el sitio es legítimo y no falso.
- Use la tecnología para reducir los riesgos — Muchos proveedores de servicios de Internet y de correo electrónico, al igual que distintos software, usan filtros para correo spam y otras tecnologías para identificar y borrar a diario miles de millones de correos spam. Algunas tecnológicas innovadoras pueden incluso detectar y bloquear potenciales correos de phishing.

Qué hacer en caso de problemas

Para reportar acosos cibernéticos o posibles pedófilos:

- Contacte a su escuela u organización comunitaria, si su hijo está siendo acosado en línea por otro estudiante o compañero de clase.
- Llame a la Policía local; si la amenaza es inmediata, llame al número de emergencias.
- Contacte la CyberTipline al 800-843-5678 (para español, presione 5) en EE.UU. o vaya a www.cybertipline.com, sitio asociado con la organización Centro Nacional para Niños Perdidos y Explotados (National Center for Missing & Exploited Children).

Para reportar phishing:

- Reenvíe el correo electrónico a su proveedor de servicio de Internet.
- Presente una queja en la Agencia local de Protección al Consumidor.
- Contacte a la compañía que está siendo falsamente representada en el correo electrónico. Tal vez ésta tenga una dirección especial para tales informes.

Si cree que es víctima de robo de identidad:

- Hable con el departamento de seguridad o fraude de sus bancos o instituciones financieras, así como de otros establecimientos donde utiliza regularmente su tarjeta de crédito.
- Cambie las contraseñas de sus cuentas en línea.
- Obtenga una copia de su informe de crédito (sin costo para víctimas de robo de identidad), solicite una alerta de fraude y pida que no se otorgue crédito nuevo sin su autorización.
- Envíe todas sus solicitudes por escrito y guarde las copias. Cuando reciba sus informes de crédito, busque cuidadosamente cualquier consulta que usted no haya iniciado, cuentas que no haya abierto y deudas sin explicación.

Respalde sus archivos:

- Ningún método de seguridad es completamente infalible. Por ende, es importante que usted respalde sus archivos más importantes periódicamente, antes de tener un problema. Aprenda cómo en www.microsoft.com/latam/protect.

Recursos Útiles:

- www.microsoft.com/latam/protect
- www.navegaprotegido.org

0409 Part No. 098-109858