Consejos para su seguridad y protección en línea

La Dirección de Asuntos Educativos y Culturales del Departamento de Estado de los EE.UU. toma muy en serio su seguridad y protección en línea. Al utilizar las redes sociales, el correo electrónico e Internet, por favor tome en cuenta los siguientes consejos de seguridad:

1. Nunca transmita datos personales. Nunca ponga su dirección de correo electrónico ni número de teléfono en ningún espacio público, tales como la página de sus datos personales, un blog, foros, ni leyendas de fotografías.

2. Si usted es miembro de una red social, preste mucha atención a sus medidas de privacidad, las cuales le permiten decidir cuánta información personal va a revelar y a quién.

3. Piense bien qué va a publicar en las redes sociales. Antes de publicar fotos, videos o texto, pregúntese si a usted le avergonzaría que su familia o su empleador llegaran a ver esa información.

4. Antes de añadir un *widget* (aplicación que puede compartirse con otros electrónicamente) a su perfil, piense si usted desearía que los creadores de la aplicación tuviesen acceso a la página de su perfil e información sobre sus actividades en la red social. Tenga en cuenta que, en general, la red social no tiene ningún control sobre esas aplicaciones. Por lo tanto, actúe con discreción al usar esos medios.

5. Notifique cualquier uso indebido del reglamento del sitio web a los administradores del mismo. Cualquier sitio web o red social de buena reputación tendrá una forma de denunciar los abusos.

6. El correo electrónico puede servir para difundir programas dañinos u obtener sus datos personales con el propósito de cometer fraude. Para protegerse usted y proteger las computadoras que utiliza, siga las directrices que se indican a continuación:

- Desconfíe de los mensajes electrónicos no solicitados o de las llamadas telefónicas de quienes solicitan información personal. Si un desconocido dice pertenecer a una organización legítima, trate de verificar su identidad directamente con esa organización.

- Nunca proporcione información personal ni financiera (números de tarjetas de crédito, números de identificación personal o PIN) cuando responda a correos electrónicos o llamadas telefónicas que usted no haya iniciado.

- No envíe información personal ni financiera a través de Internet antes de comprobar que el sitio web es seguro. (Las direcciones protegidas comienzan con "https://")

- Preste atención a la dirección del sitio web, ubicada en la parte superior de la pantalla. Los sitios web malintencionados pueden parecer idénticos a los sitios legítimos, pero en la dirección puede haber una ortografía distinta o un dominio diferente (por ejemplo, ".com" en vez de ".net").

- Proteja su propia computadora y otras que utilice. Para ello, escanee todos los medios extraíbles; por ejemplo, las unidades flash, los CD o los DVD, en busca de virus antes de abrir los archivos que estén en esos medios. Asimismo, escanee todos los archivos adjuntos que reciba por correo electrónico antes de abrirlos.

- No acepte ni abra archivos ejecutables (indicados por un nombre de archivo que termina en ".exe") que reciba por correo electrónico. Esos archivos pueden ser peligrosos.