# ¡OJO!

FTC Resources for Hispanic Communities

Vol.3, No.3 October 2007
ftc.gov/espanol

*Editor's Note: This issue of ¡Ojo! provides information to help you navigate the Internet. It has tips on how to protect against spyware, recognize and avoid spam and phishing scams, and safely use social networking websites.*

## SPYWARE: WHAT IT IS AND HOW TO PREVENT IT

Have you noticed that your computer is running more slowly than normal? Are you overwhelmed by a barrage of pop-up ads or unexpected toolbars? Are icons or random error messages suddenly appearing on your screen? These may be clues that spyware is on your computer.

Spyware is software that has been installed on your computer without your knowledge or consent. It affects your ability to use your computer, sometimes by monitoring or controlling computer use or by sending you pop-up ads, redirecting your computer to websites, monitoring your Internet surfing, or recording your keystrokes to steal your personal information or identity.

To lower your risk of spyware:

- get an anti-spyware program from a vendor you know and trust and set it to scan every time you start your computer.
- delete any software programs the anti-spyware program detects that you don't want on your computer.

See *Spyware*, p.4

## SPYWARE: QUÉ ES Y CÓMO PREVENIRLO

¿Ha notado que su computadora funciona más lento que lo normal? ¿Está abrumado por el bombardeo de anuncios *pop-up* o la aparición inesperada de barras de herramientas? ¿En su pantalla aparecen repentinamente íconos u ocasionales mensajes de error? Estos problemas pueden estar indicando que usted tiene un *spyware* en su computadora.

*Spyware* es un programa que ha sido instalado en su computadora sin su conocimiento ni consentimiento y que afecta el uso y rendimiento de su computadora. A veces puede hacer un monitoreo o controlar el uso de la computadora o enviarle anuncios *pop-up*, redirigir su computadora a sitios Web, monitorear su navegación del Internet o registrar lo que usted escribe en el teclado para robarle su información personal o su identidad.

Para disminuir el riesgo del *spyware*:

- Compre un programa *anti-spyware* en una tienda o proveedor conocido y confiable y prográmelo

Vea *Spyware*, p.4

INSIDE...



*To file a complaint, visit **ftc.gov/complaint** or **ftc.gov/queja**.*

*To receive this newsletter electronically, or to be added to or removed from our mailing list, email **HispanicOutreach@ftc.gov**.*

## A PARENT'S GUIDE TO SOCIAL NETWORKING SITES

In just a few years, social networking websites have changed the way many kids and adults communicate online. These sites encourage and allow people to exchange information about themselves, and use blogs, chat rooms, email, or instant messaging to communicate with others around the corner or around the world. But while social networking sites can increase a person's circle of friends, they also can pose risks if they are not used safely.

So what can parents do to limit their kids' exposure to people who may have less-than-friendly intentions?

- Help your kids understand what information they should keep private. Tell them why it's important to keep some things about themselves, family members, and friends to themselves.
- Use privacy settings to restrict who can access and post on your child's website.
- Remind your kids that once they post information online, they can't take it back.
- Tell your kids to trust their gut if they have suspicions. If they feel threatened by someone or uncomfortable because of something online, encourage them to tell you.

To learn more, go to OnGuardOnline.gov/socialnetworking. Test your social networking smarts with your kids by playing the Buddy Builder game.

OnGuard Online | YOUR SAFETY NET™

## UNA GUÍA PARA PADRES SOBRE SITIOS WEB DE REDES SOCIALES

Solamente en unos pocos años, los sitios Web de redes sociales han cambiado la forma de comunicarse de muchos niños y adultos. Estos sitios promueven y permiten que las personas intercambien información personal, usen *blogs*, salas de chateo, e-mail o mensajes instantáneos para comunicarse con el vecino de enfrente o con el mundo entero. Pero si bien es cierto que las redes sociales en línea pueden ampliar el círculo de amigos de una persona, también pueden plantear riesgos cuando no se usan con cuidado.

Entonces, ¿qué es lo que pueden hacer los padres para que sus hijos limiten su exposición a aquellas personas con intenciones poco amigables? Ante todo, ya que muy probablemente sus hijos estén navegando o participando de redes sociales en inglés, cuando les hable de este tema refiérase a *social networking* y trate de aprenderse el vocabulario específico.

- Hable con sus hijos para ayudarlos a comprender cuál es la información que no deben compartir con nadie. Explíqueles la importancia de mantener algunos datos privados — información sobre sí mismos y de sus familiares y amigos, por ejemplo.
- Utilice las funciones de privacidad para limitar quien puede acceder el sitio Web de su hijo y colocar información.
- Recuérdeles a sus hijos que una vez que coloquen información en línea no podrán quitarla.
- Dígales a sus hijos que si tienen alguna sospecha confíen en sus propios instintos y que si cuando están en línea se sienten amenazados por alguna persona o se sienten incómodos con algo que ven en línea, se lo digan a usted.

Para aprender más sobre este tema, visite en Internet AlertaenLinea.gov/redes_sociales. Compruebe sus conocimientos sobre las redes sociales junto a sus hijos participando del juego Fábrica de Amigos.

## AVOID THE LURE OF SPAM AND PHISHING EMAILS

More and more, consumers are relying on email to communicate — at home and at work. And although email has become a valuable tool for keeping in touch, it is also being used to scam people. Many Internet service providers offer tools to block spam, but it also pays to know the signs of a scam so you can recognize it if and when you see it. For example, "phishing" emails try to trick you into giving out your personal information. These emails look like they are from a business you might deal with — for example, an Internet service provider (ISP), bank, online payment service, or even a government agency. The message usually says that you need to "update" or "validate" your account information. It might threaten some dire consequences if you don't respond. Don't take the bait. Legitimate companies don't ask for this information via email. Forward the message to the authorities at spam@uce.gov and then delete it.

To avoid getting hooked by spam or phishing scams:

- Be cautious about opening attachments or downloading files from emails you receive, especially if you don't expect them and don't know the sender.
- Never email financial information, and never click on links in email or pop-up ads that ask for personal or financial information.
- If you are directed to a website to update your information, verify that the site is legitimate by calling the company directly, using contact information from your account statements.
- Use anti-virus and anti-spyware software, as well as a firewall, and update them all regularly.

For more, visit OnGuardOnline.gov/spam.

## EVITE LOS MENSAJES ELECTRÓNICOS SPAM Y PHISHING

Cada vez más, los consumidores usan el correo electrónico para comunicarse — en sus casas y en sus trabajos. Y aunque el e-mail se ha convertido en una valiosa herramienta para mantenerse en contacto, también está siendo utilizado para estafar a otras personas. Muchos proveedores de servicio de Internet ofrecen he- rramientas para bloquear el *spam*, pero también vale la pena reconocer los indicios de una estafa. Por ejemplo, los textos de los mensajes electrónicos "*phishing*" intentan engañarlo para que revele su información personal. Parecen provenir de negocios con los que usted podría tener una relación comercial — como un proveedor de servicio de Internet, su banco, servicio de pago en línea o una agencia del gobierno. Usualmente, el texto del mensaje dice que es necesario que usted "actualice" o "valide" la información de su cuenta. Es posible que el incluya algún tipo de amenaza sobre las terribles consecuencias que puede sufrir si no responde. No muerda el anzuelo. Las compañías legítimas no piden esta información vía e-mail. Reenvíe el mensaje a spam@uce.gov y elimínelo.

Para evitar que lo pesquen con estas estafas:

- Tenga cuidado al abrir archivos adjuntados a los mensajes, especialmente si no los está esperando y si desconoce al remitente.
- Nunca envíe información financiera por email, y nunca haga clic sobre los enlaces de un e-mail ni de los anuncios *pop-up* que le piden información personal.
- Si es dirigido a un sitio Web para actualizar su información, verifique que se trata de un sitio legítimo llamando a la compañía y utilizando la información de contacto que aparece en sus resúmenes de cuenta.
- Use programas antivirus, *anti-spyware* e instale un *firewall* y actualícelos con regularidad.

Para más información sobre este tema, visite AlertaenLinea.gov/spam.

*Spyware* from p.1

- update your operating system and Web browser software, and set your browser security high enough to detect unauthorized downloads.
- download free software only from sites you know and trust. Some free software downloads — like games, screen savers, and e-cards — often can bundle other software, including spyware.
- don't click on links in spam that claim to offer anti-spyware software, and don't click on any links inside pop-up windows; you may be installing spyware unintentionally.

For more tips on how to avoid spyware, visit OnGuardOnline.gov/spyware.

*Spyware* de p.1

para que haga un escán de su computadora cada vez que la inicie.

- Elimine los programas detectados por el programa *anti-spyware* que no desee tener instalados en su computadora.
- Actualice su sistema operativo y su navegador de Internet y configure la función de seguridad en un nivel suficientemente alto para detectar las descargas no autorizadas de programas o archivos.
- Descargue programas gratuitos ofrecidos únicamente por sitios conocidos y confiables. Algunos programas que pueden descargarse gratuitamente — tales como juegos, fondos o protectores de pantalla y tarjetas electrónicas — a menudo pueden acarrear otros programas, incluso *spyware*.
- No haga clic sobre los enlaces incluidos en mensajes de tipo *spam* que dicen ofrecer un programa *anti-spyware*, y tampoco haga clic sobre los enlaces que se encuentran en las ventanas de aparición automática o *pop-up* ya que podría instalar un *spyware*.

Para consultar más recomendaciones sobre cómo evitar el *spyware*, visite AlertaenLinea.gov/spyware.

## Reach Out in your Community

### October
- National Cyber Security Awareness Month: help others stay safe online
  www.OnGuardOnline.gov

### November
- Weight loss and miracle cure scams
- Franchise and business opportunity scams
  www.ftc.gov/bizopps

### December
- Safe holiday shopping
- Gift cards
- Prepaid calling cards

For more ideas, visit ftc.gov/reachout.

Email HispanicOutreach@ftc.gov to become an FTC Hispanic outreach partner.

## Enseñe en su Comunidad

### Octubre
- Mes Nacional Informativo sobre Ciber-seguridad: ayude a otras personas a mantenerse seguras en línea
  www.AlertaenLinea.gov

### Noviembre
- Estafas de pérdida de peso y curas milagrosas
- Estafas de franquicias y oportunidades de negocio
  www.ftc.gov/trabajoencasa

### Diciembre
- Compras navideñas y de fin de año sin riesgos
- Tarjetas de regalo
- Tarjetas de llamadas prepagadas

Para consultar más ideas al respecto, visite ftc.gov/ensena.

Escriba a HispanicOutreach@ftc.gov para unirse a la FTC en la lucha contra el fraude.