## PROTEGE TU PRIVACIDAD

Si crees que hay "Spyware" en tu computadora, trata de usar una más segura cuando busques ayuda. Puede ser más seguro usar la de una biblioteca, la de un amigo, centro comunitario o un cibercafé.

Si sospechas que alguien tiene la contraseña de cualquiera de tus cuentas, ve a una computadora a la que esta persona no tenga acceso y cámbiala. Sólo revisa esa cuenta desde una computadora a la que esa persona no puede ingresar. Las contraseñas más seguras son las que tienen por lo menos ocho caracteres y usan una combinación de letras y números.

Si sospechas que una persona agresora puede ingresar a tu correo electrónico o mensajes instantáneos (IM por las siglas en inglés), considera crear cuentas de correo electrónico o mensajes instantáneos adicionales en una computadora segura. Busca en la red cuentas de correo gratis y considera usar nombres e información que no te identifiquen (ejemplo: gatoazul@correo.com y NO uses TuNombreReal@correo.com).También, lee cuidadosamente las pantallas de registro para que puedas escoger que no se te incluya en los directorios en línea de nadie.

Recuerda que muchos teléfonos no son más que minicomputadoras. Las personas que acechan pueden poner programas de "Spyware" en los celulares y otros aparatos portátiles para registrar cada mensaje de texto enviado y cada número marcado. Asimismo, si saben tu contraseña, alguien se puede conectar a tu cuenta telefónica, bancaria u otras cuentas en línea. ¡Así que mantén tus contraseñas secretas y cámbialas con frecuencia!

## RECURSOS

Coordinadora Paz para la Mujer
Coalición Puertorriqueña contra la Violencia Doméstica y Agresión Sexual
www.pazparalamujer.org

SafetyNet:
National Safe & Strategic Technology Project
www.nnedv.org/projects/safetynet

Federal Trade Commission
www.OnGuardOnline.gov

Fundación Ricky Martin
www.navegaprotegido.org

Negociado Especial de Investigaciones
www.justicia.gobierno.pr/nie/

National Online Resource Center on Violence Against Women, Special Collection: Technology Safety
www.vawnet.org

GetNetWise
www.getnetwise.com

Pew Internet & America Life Project
www.pewinternet.org

Bureau of Justice Statistics, "Stalking Victimization in the United States", enero 2009
www.ojp.usdoj.gov

Internet World Stats, United States of America: "Internet Usage and Broadband Usage Report"
www.internetworldstats.com

Internet Keep Safe Coalition
www.ikeepsafe.org

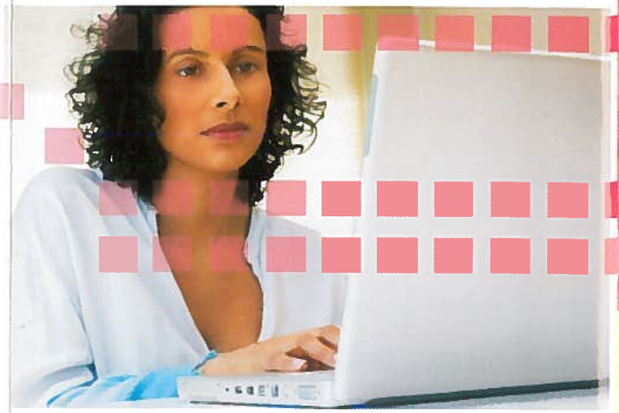
i-SAFE
www.i-safe.org

National Center for Missing and Exploited Children
www.missingkids.com; www.netsmartz.org

National Crime Prevention Council
www.ncpc.org

National Cyber Security Alliance
www.staysafeonline.org
Staysafe
www.staysafe.org

Wired Safety
www.wiredsafety.org




Referencias

Este material en su mayoría fue adaptado de la hoja "Adolescentes Tecnisabios", creado en mayo del 2007 por el Proyecto SafetyNet del National Network to End Domestic Violence.

La sección "Tu seguridad está en juego" fue extraída, traducida y adaptada de la publicación "Social Networking Sites: Safety Tipos for Tweens and Teens" de la Comisión Federal del Consumidor.



Revisado en el 2012.

Esta publicación ha sido posible gracias al auspicio del United States Department of Justice Violence Against Women Act, USDOJ-VAWA Contrato: 2012 MUAX0019. Las opiniones expresadas en esta publicación son de las/os autoras/es y no reflejan las opiniones del Departamento de Justicia de los EE.UU.



COORDINADORA PAZ PARA LA MUJER
Apartado 193008, San Juan PR 00919-3008
Tel. (787) 281-7579, (787) 777-0738
Fax: (787) 767-6843
Correo electrónico: info@pazparalamujer.org

Paz para la Mujer | Fan Page: Paz Mujer
pazparalamujer YouTube pazmujer's channel


COORDINADORA PAZ PARA LA MUJER

# ACECHO cibernético

## ¿Cómo protegernos en el ciberespacio?

**Coordinadora Paz para la Mujer, Inc.**
**Coalición Puertorriqueña contra la Violencia Doméstica y la Agresión Sexual**

www.pazparalamujer.org

# BLOGS y REDES SOCIALES

**¿HAS PUESTO TU PERFIL EN UN SITIO ELECTRÓNICO DE INTERCAMBIO SOCIAL COMO "MYSPACE", "FACEBOOK," O "TWITTER" O EN UNA DE CITAS O DE EX ALUMNOS EN INTERNET?**

¿Registraste tu perfil como privado? Si no, cualquiera que visite esa página, puede ver tu información personal, incluyendo oficinas de admisión universitarias, maestros/as, parientes, empleadores/as potenciales y hasta acechadores/as.

**¿USAS CORREO ELECTRÓNICO GRATIS, UN "BLOG", MENSAJES INSTANTÁNEOS O COMPARTES MÚSICA O FOTOS EN LÍNEA?**

Cuando te registraste para ese servicio, ¿diste tu nombre, edad, sexo, ciudad en que vives y tus pasatiempos? Si es así, la compañía que obtuvo tu información puede haberla puesto en línea públicamente (para que todas las personas la vean). Muchas veces puedes escoger que no te registren en un directorio o puedes dar información limitada (por ejemplo, sólo tu nombre de pila o un nombre falso).

**¿HAS TOCADO CON LA BANDA ESCOLAR, HAS PUESTO TUS TRABAJOS EN UNA EXHIBICIÓN DE ARTE O HAS ESTADO EN UN EQUIPO DEPORTIVO?**

Si es así, pueden poner en internet tu nombre, detalles personales e información de contacto. Algunas páginas quitan la información si tú lo pides; pero si la página se archiva, tu información en realidad no se borra. Mientras más rápido eliminen tu información, mejor.

**¿CÓMO SÉ QUE ALGO ESTÁ YA EN EL INTERNET?**

Si tú lo puedes encontrar, alguien más también lo puede hacer. Busca en Internet tu información y fotos personales. Puedes comenzar en sitios como Google, Yahoo, Classmates.com, YouTube, y Flickr.

Busca en los sitios electrónicos para grupos y lugares con los que puedas estar conectado/a: tu escuela, clubes, empleo, grupo de iglesia, equipo deportivo, grupos comunitarios y voluntarios, etc.

# ARCHIVO

Las páginas electrónicas pueden archivarse o esconderse (en caché) así que la gente puede seguir viendo el contenido viejo aunque la página desaparezca o cambie. Esto significa que la información publicada en Internet puede estar en línea por mucho tiempo – quizás para siempre. ¡El Archivo de Internet (www.archive.org) tiene 55 mil millones de páginas electrónicas!

**OTRAS FORMAS EN LAS QUE TU INFORMACIÓN LLEGA AL INTERNET:**

Cuando haces una compra, la tienda te pide el número de teléfono o tu código postal y tus datos se registran en una base de datos. La tienda puede luego vender tu información a un mayorista de datos que la pone en un directorio en línea.

Un amigo/a o compañero/a de clase pone en línea tu información o fotos. Quizás un familiar pone un álbum de fotos de familia en el que tú estás.

Muchos registros públicos se ponen en internet, así que si tienes licencia de conducir, te han expedido infracciones de tráfico o has estado en el tribunal, tu nombre, dirección y otros datos personales pueden estar disponibles en línea en el sitio electrónico del tribunal o del gobierno.

**¿RECIBES CIENTOS DE MENSAJES DE TEXTO O DE VOZ DE ALGUIEN CON QUIEN NO INTERESAS HABLAR?**

Si estás siendo acechado/a por vía telefónica o mensaje de texto, tienes opciones:

Puedes hablar con tu compañía de teléfono para bloquear llamadas y otros servicios o para cambiar tu número.

Puedes hablar con la policía para saber si hay evidencia para una querella de acecho u hostigamiento. Las llamadas y mensajes de texto de acecho o acoso son ilegales en Puerto Rico y puede constituir un delito grave (bajo la Ley Núm. 284 del 21 de agosto de 1999, Ley contra el Acecho en Puerto Rico).

**¿TE PARECE QUE HAY ALGUIEN QUE SABE SOBRE CADA CORREO QUE HAS ENVIADO O TODO LO QUE HAS ESCRITO EN MENSAJES INSTANTÁNEOS EN LÍNEA?**

Puede que haya alguien usando tu conexión personal con tu programa de mensajes instantáneos en Internet o que haya cambiado la programación de tu correo para que secretamente les envíe copias. También es posible que alguien haya instalado un programa de "Spyware" de espionaje en tu computadora. Las personas que acechan pueden instalar "Spyware" aunque no tengan acceso físico a tu computadora o equipo manual. Algunas de las personas que acechan pueden entrar a tu computadora desde otra localización por Internet. Algunas personas pueden enviar "Spyware" como un archivo adjunto que se instala automáticamente cuando abres el correo o cuando inicialmente lo ves en la bandeja de entrada. Otros pueden enviar un correo o mensaje instantáneo de una tarjeta, juego de computadora u otro artificio para instigarte a que abras un adjunto o que entres a un enlace.

Una vez que tienes el "Spyware" en tu computadora, éste puede correr sigilosamente y es difícil de detectar o de eliminar por completo. Si la persona que instaló el "Spyware" tiene acceso físico a tu computadora, se puede usar una combinación clave especial para hacer que salga una pantalla secreta de ingreso al programa. Luego de entrar la contraseña, el programa de "Spyware" hace que la persona vea el registro de todas las actividades en tu computadora, desde la última vez que te conectaste, incluyendo los correos que enviaste, lo que imprimiste, sitios electrónicos visitados, búsquedas que hiciste y más. Aun sin tener acceso físico a tu computadora, las personas que acechan pueden programar el spyware para que tome fotos de tu pantalla de computadora cada cierto número de segundos y se las envíe por Internet sin que tú lo sepas.

# TU SEGURIDAD ESTA EN JUEGO

Algunas sugerencias para navegar con seguridad.

1. Investiga cómo funcionan algunas páginas de Internet antes de registrarte. Algunas páginas permiten solo a una comunidad de usuarios/as definida acceder el contenido; otras permiten a todo el mundo mirar lo que se postea.
2. Piensa en mantener algún control sobre la información que coloques. Considera restringir el acceso a tu página a un selecto grupo de personas, por ejemplo, a amistades de la escuela, universidad, club, equipo, grupos comunitarios, o a tu familia.
3. Mantén la información solo para ti. No coloques tu nombre completo, número de seguro social, dirección, número de teléfono, o números de cuentas bancarias o tarjetas de crédito y no coloques la información de otras personas tampoco. Ten precaución al colocar información que puede ser utilizada para identificarte o localizarte fuera del Internet. Esto puede incluir el nombre de tu escuela o universidad, equipo deportivo, clubs o donde trabajas o jangueas.
4. Asegúrate que tu nombre de usuario no diga demasiado sobre ti. No utilices tu nombre, tu edad, o tu pueblo. Aunque pienses que tu nombre de usuario es anónimo, no se necesita a una persona genio para atar cabos e identificar quién eres y dónde se te puede encontrar.
5. Coloca información con la que te sientas cómodo/a que otras personas vean y sepan sobre ti. Muchas personas pueden ver tu página, incluyendo tus familiares, maestros/as, la policía, la universidad o tu empleo presente o futuro.
6. Considera el no colocar tu foto. Puede ser alterada y publicada sin tu consentimiento. Si colocas una, pregúntate si estuvieras dispuesta/o a que todo el mundo la viera.
7. Coquetear con personas extrañas en el internet puede tener consecuencias serias. Algunas personas mienten sobre quienes son realmente, así que nunca sabes con certeza con quién te estás comunicando.
8. Ten cuidado si una nueva amistad en internet quiere conocerte en persona. Antes que decidas conocer a alguien, investiga: Pregunta si algunas de tus amistades conocen a la persona, y verifica qué información puedes extraer del Internet a través de motores de búsqueda. Si decides conocerle en persona, sé lista/o: Conócele en un lugar público, durante el día, con amistades de confianza. Déjale saber a alguien donde estarás y cuando esperas regresar.
9. Confía en tus instintos si tienes sospechas. Si te sientes amenazada/o o incómodo/a a causa de algo en el internet, déjaselo saber a un adulto/a en quien confíes e infórmalo a la policía y a la red social. De esta forma puedes prevenir que otra persona se convierta en víctima.