safehorizon

Tech Safety

For victims of crime, abuse, domestic violence and stalking

Computers, tablets, phones, apps, and social network sites impact how we connect to the world every day. They can offer help, valuable resources, and support if you are experiencing domestic violence or stalking. As you use technology and plan for your safety in these situations, it is also important to be aware of the risks. The information below can help you to use technology in more informed, safer ways.

These tips provide suggestions for you to be aware of. But you are the only one who can decide what is best for you and your safety.

Online Safety

Did you know?

- Information that is posted online is never private.
- Your computer can be monitored by someone else without your knowledge or consent.
- Your computer's online browser history can never be completely removed. Clearing or changing the browser history on your personal computer may also create a safety risk.
- Your emails and instant messages can be monitored, intercepted, and retrieved by someone else.
- Your computer's webcam can be turned on remotely and used by others to spy on you without your consent.
- Spyware, a type of software that can track and monitor your information and activity through your computer or phone, can be installed onto your device from the outside (without your knowledge or consent), through email attachments, links, and other means.

Consider ways to stay safer:

- Using safer computers or devices
  - If you believe someone has access to your computer or may be monitoring your use, consider using another computer or device that the person does not have access to. Safer computers may be at libraries, shelters, internet cafes, work, or a computer technology center.
- Limiting the personal information that you share about yourself online
  - There is no way to be sure your information is completely private. Be conscious of what you are sharing online and who may be able to see it or share it with others.
  - If there is information about you on the internet that you are uncomfortable with, consider taking steps to remove the information by contacting the websites directly.
- Creating alternative email accounts using a safer computer
  - Someone monitoring your activity may have access to your email account. Consider setting up an entirely new email account that is not connected to the one you currently use. You can use this new account for communications about your safety and sensitive matters. Keep your previous account in order to maintain the appearance that nothing has changed, and use it for other kinds of communication.
- Changing your passwords and usernames

  Using a safe computer, consider changing the usernames and passwords of your online accounts.
  - It may be safer to create a new username that is different from your name so you cannot be easily identified.
  - You may want to create different passwords for every account using letters, numbers, characters, and words or dates that others would not associate with you. A more secure password may look something like: C0mp$t3r!.
  - It may be more secure to only use these new usernames and passwords on safe computers or devices that cannot be monitored.
- Setting up 2-step verification on all of your online accounts can help prevent unauthorized access by adding an extra level of security to logging in.
- Keeping computers with webcams out of the personal spaces of your home or workplace, covering the lens of the camera, pointing it towards a wall, and making sure that your webcam is off when you are not using it.
- Being cautions when clicking on unknown links and opening emails from someone you feel may be monitoring you (or from unknown addresses) even if the messages look legitimate.
- Installing a firewall on your computer, as well as anti-virus software.

Networking Safely on Social Media

Did you know?

- Once something is posted on social media, it is no longer under your control.
- Posts on social media, including personal information and photos, can potentially be viewed by anyone, even those who are not directly connected (or "friends") with you.
- Personal information that is commonly shared on social media may allow someone else to know your activity and movement both online and offline.

Consider ways to stay safer:

- Only posting things that you would like the public to see.
- Protecting your personal information such as pictures, videos, phone numbers, email addresses, birth dates, the schools you have attended, places you have worked, and current locations where you hang out.
- Keeping your social media passwords private and not sharing them with others.
- Logging off when you are not actively using your account to prevent unauthorized access.
- Asking your friends, family, and acquaintances not to share any personal information about you, tag you in photos, or share your location on social media.
- Being aware of and understanding privacy settings. Setting your profile to private does not necessarily mean that all of your information is truly private. Checking these settings frequently could also be helpful, as sites often change their policies.
- Turning off and disabling location services such as location tracking, tagging, and checking-in features.

Phone Safety

Did you know?

- Your cell phone use can be monitored by someone else without your knowledge or consent.
- Your call and text message history can be recovered and viewed by someone else.
- Cell phones have the ability to track and monitor your exact location in real time.

Consider ways to stay safer:

- Reviewing your phone's settings
  - Making sure that your phone is not connected to other devices
  - Creating a passcode for accessing your phone
  - Disabling your phone's auto-answer option, if it has one
  - Disabling or turning off location and navigation services as well as Bluetooth, and using caution when using any mobile apps that utilize these features
- Deleting all apps that you are not familiar with, do not use, or do not understand
- Asking your phone service carrier for information about location services or apps
- Finding out if it is possible to take the batteries out of your phone to prevent your phone from transmitting signals and data
- Getting a new phone whose account information is not known to anyone; a donated or "pay as you go" cell phone may be a safer alternative

If you believe that an abusive partner or someone else may be monitoring your activity, harassing you, or stalking you through technology or the internet, help is available.

For more information and suggestions for staying safe with technology, please visit: www.safehorizon.org/techsafety

The National Domestic Violence Hotline Tech and Social Media Safety
http://dev.thehotline.org/help/tech-social-media-safety/

The National Network to End Domestic Violence Technology Safety Blog
http://techsafety.org/

Safe Horizon's Hotline offers free 24/7 help:
800.621.HOPE (4673) TDD hotline: 866.604.5350
Reach out for help if you feel unsafe or if you need information or tips on how to stay safe.

safehorizon
moving victims of violence from crisis to confidence

safehorizon

La seguridad en la tecnología

Para vîctimas de crimen, abuso, violencia doméstica y acoso

Las computadoras, las tabletas, los teléfonos celulares, las aplicaciones, y las redes sociales, impactan la manera en que nos conectamos con el mundo cada día. También nos pueden ofrecer ayuda, recursos valiosos, y apoyo para las víctimas de violencia doméstica y acoso. En la medida en que usamos la tecnología y planeamos nuestra seguridad, es muy importante estar consciente de los riesgos. La información presentada a continuación te puede ayudar a hacer uso de la tecnología de una manera más informada y segura.

Estos consejos te proveen sugerencias, sin embargo solo tú eres quien decide lo que es mejor para tu seguridad.

Seguridad en la internet

¿Sabías?

- La información que publicas en la internet nunca es privada.
- Tu computadora puede ser monitoreada por otra persona sin tu conocimiento o consentimiento.
- La historia de navegación en internet de tu computadora nunca puede ser borrada completamente. Borrar o limpiar la historia de navegación puede ocasionar un riesgo a tu seguridad.
- Tus correos electrónicos y mensajes instantáneos pueden ser monitoreados, interceptados, y recuperados por alguien más.
- La cámara de tu computadora puede ser activada remotamente y usada por otros para espiarte sin tu consentimiento.
- Spyware, un tipo de software que puede rastrear y monitorear tu información y actividad a través de tu computadora o teléfono, puede ser instalado en tu máquina desde el exterior sin tu conocimiento o consentimiento, a través de anexos a correos electrónicos, enlaces u otros medios.

Considera maneras para mantenerte a salvo:

- Utiliza computadoras o aparatos electrónicos más seguros.
  - Si piensas que alguien ha tenido acceso a tu computadora o puede estar monitoreando su uso, considera utilizar otra computadora o aparato electrónico al que la persona en cuestión no tenga acceso. Computadoras más seguras se pueden encontrar en las bibliotecas, los cafés internet, en tu lugar de trabajo, o un centro de tecnología en computación.
- Limita la cantidad de información personal que compartes en internet.
  - No existe la manera de poder asegurar que tu información está completamente privada. Sé consciente de qué estás compartiendo en internet, y quién puede estarlo viendo y compartiendo con otros.
  - Si existe información sobre tu persona en internet con la que te sientes incómodo, considera tomar pasos para remover esta información, contactando a la página de internet directamente.
- Crea cuentas de correo electrónico alternativas utilizando una computadora más segura.
  - Si alguien monitorea tu actividad, puede tener acceso a tu cuenta de correo electrónico. Considera crear una cuenta de correo electrónico nueva que no esté conectada a la que utilizas actualmente. Puedes utilizar esta nueva cuenta para las comunicaciones que contengan aspectos de tu seguridad y asuntos delicados. Conserva tu cuenta anterior para mantener la apariencia de que nada ha cambiado, y utilízala para otros tipos de comunicación.
- Cambia tu nombre de usuario y contraseñas.

  Usando una computadora segura, considera cambiar los nombres de usuario y las contraseñas de tus cuentas en internet.
  - Es más seguro crear un nombre de usuario que sea diferente a tu nombre, de manera que no seas fácilmente identificado
  - Es mejor crear diferentes contraseñas para cada cuenta, usando letras, números, caracteres, y palabras o fechas que otras personas no puedan asociar contigo. Una contraseña segura puede ser la siguiente: Comp$t3r!.
  - Es más seguro utilizar estos nombres de usuario y contraseñas en computadoras y aparatos seguros que no puedan ser monitoreados.
- Programar un sistema de verificación de identidad de 2 pasos en cada una de tus cuentas de internet puede ayudar a prevenir el acceso no autorizado, al añadir un nivel adicional de seguridad para abrirlas.
- Mantén las computadoras con cámaras web fuera de los espacios personales de tu hogar o lugar de trabajo. Cubre el lente de la cámara, dirígela hacia una pared, y asegúrate de que tu cámara esté apagada cuando la estés usando.
- Ten precaución cuando vayas a un link desconocido y cuando abras correos electrónicos de alguien que tu creas pueda estar monitoreándote (o de direcciones desconocidas) inclusive si los mensajes parecen legítimos.
- Instala un programa de protección en tu computadora, así como un software antivirus.

Interactúa de manera segura en las redes sociales

¿Sabías?

- Una vez algo se publica en una red social, ya no está bajo tu control.
- Toda publicación en redes sociales, incluyendo tu información personal y fotos, puede potencialmente ser vista por cualquier persona, incluyendo personas que no están directamente relacionadas contigo ni son “tus amigos“.
- La información personal que es comúnmente compartida en las redes sociales puede permitirle a otros conocer tus actividades y movimientos tanto en la red como por fuera de ella.

Considera maneras para mantenerte a salvo:

- Sólo publica aquello que te gustaría que el público viera.
- Protege tu información personal como fotografías, videos, números telefónicos, direcciones de correo electrónico, fechas de nacimiento, escuelas a las que has atendido, lugares en donde has trabajado, y lugares que frecuentas.
- Mantén tus contraseñas de redes sociales privadas y no las compartas con otros.
- Cierra tu cuenta cuando no estás usándola para prevenir el acceso no autorizado.
- Solicítale a tus amigos, familia y conocidos no compartir tu información personal, no identificarte en las fotos ni compartir tu ubicación.
- Mantente informado de las especificaciones de privacidad de las páginas de redes sociales. Programar tu perfil como privado, no necesariamente significa que toda tu información está completamente privada. Revisar estas especificaciones de privacidad a menudo, puede también ser muy conveniente, pues cambian con regularidad.
- Apaga y desactiva los servicios de ubicación como los de rastreo, identificación y registro.

Seguridad telefónica

¿Sabías?

- El uso de tu teléfono celular puede ser monitoreado por alguien más sin tu conocimiento o consentimiento.
- La historia de tus llamadas o mensajes de texto puede ser recuperada y vista por alguien más.
- Los teléfonos celulares tienen la habilidad de rastrear y monitorear tu ubicación exacta en tiempo real.

Considera maneras para mantenerte a salvo:

- Revisa las especificaciones de tu teléfono:
  - Asegúrate que tu teléfono no está conectado a otros aparatos.
  - Crea una contraseña para accesar tu teléfono.
  - Desactiva la opción de contestador automático de tu celular, si lo tiene
  - Desactiva o apaga los servicios de ubicación y navegación así como el Bluetooth, y ten precaución al usar cualquier aplicación que utilice estas opciones.
- Borra toda las aplicaciones que desconoces, no utilices o no comprendas
- Pregúntale a tu proveedor de servicio sobre información acerca de los servicios de ubicación o aplicaciones.
- Averigua si es posible sacar las baterías de tu teléfono para prevenir que tu teléfono transmita señales y datos.
- Obtén un nuevo teléfono cuya cuenta no sea conocida; un teléfono donado o pre-pago puede ser una alternativa más segura.

Si piensas que un compañero abusivo o cualquier otra persona puede estar monitoreando tu actividad o acosándote a través de la tecnología o la internet, existe ayuda.

Para más información y sugerencias para mantenerte seguro al hacer uso de la tecnología, por favor visita: www.safehorizon.org/techsafety

The National Domestic Violence Hotline (Línea Nacional de Violencia Doméstica) Tech and Social Media Safety (Seguridad en las redes sociales y la tecnología) http://dev.thehotline.org/help/tech-social-media-safety/

The National Network to End Domestic Violence (La red nacional para terminar con la violencia doméstica)

Technology Safety Blog (Blog de seguridad en la tecnología) http://techsafety.org/

La línea de ayuda de Safe Horizon ofrece ayuda gratuita las 24 horas los siete días de la semana: 800.621.HOPE (4673) Número telefónico TDD para línea de ayuda: 866.604.5350

Contáctanos si no te sientes seguro o si necesitas información o consejos sobre cómo mantenerte a salvo.

safehorizon

moving victims of violence from crisis to confidence