## El Acoso y la Tecnología

Existen un gran número de tecnologías nuevas que se están utilizando para acosar y acechar. Las herramientas que los ofensores pueden utilizar incluyen:

- Páginas de medios sociales como Facebook
- Hachear cuentas de correo electrónico de la víctima
- La instalación de spyware en la computadora de la víctima que controla la actividad de un dispositivo independiente
- Instalación de dispositivos GPS o aplicaciones en el carro o teléfono de la víctima
- La activación de teléfono de la víctima para realizar un seguimiento a través de la compañía de teléfonos celulares

Si usted cree que alguien puede estar usando la tecnología para acosarlo, amenazarlo o acecharlo, documente la actividad y repórtelo a la policía. Si usted cree que alguien le está rastreando, deje de utilizar el dispositivo/aparato que puede ponerlo en peligro.

## El Internet y los Niños

Los niños son los usuarios más vulnerables/ desprotegidos del Internet. Es importante recordar que ellos pueden ser más "conocedores de la tecnología" que las generaciones anteriores, pero pueden no darse cuenta o no estar preocupados sobre todos los riesgos asociados con las nuevas tecnologías.

El Internet también ofrece un espacio u oportunidad para que los predadores de todo tipo puedan tener acceso a los niños con facilidad. Si usted tiene o conoce niños que utilizan el internet y son capaces de usar los dispositivos/aparatos de Internet (teléfonos inteligentes, tabletas, reproductores de música, etc.), hable con ellos acerca de la seguridad en Internet y asegúrese de que la configuración de seguridad sean adecuadas para protegerlos. Por ejemplo, configurar el control parental para bloquear ciertos tipos de sitios web o para negar la descarga.

Lo más importante es hablar con ellos acerca de internet "el peligro de los extraños" para que entiendan los riesgos y cuáles son sus expectativas. (Que es lo que usted espera)

## ¿Quién Puede Ayudar?

La Unidad de Servicios para Víctimas en la Oficina del Sheriff del Condado de Travis le puede ayudar con información sobre el estado de su caso, Derechos de las Víctimas del Crimen, Compensación a las Víctimas del Delito, como navegar el sistema de justicia criminal, y pueden dar referencias a profesionales u organizaciones adecuadas que ayudan de acuerdo a sus necesidades específicas.

## Recursos

TX Office of the Attorney General's Cyber Safety website:
www.texasattorneygeneral.gov

Federal Trade Commission Internet Safety website:
www.consumer.ftc.gov

WiredSafety is a US charity operating through volunteers. It is the largest and oldest online safety, education, and help group in the world.
www.WiredSafety.org

National Center for Missing and Exploited Children
www.netsmartz.org/

August 2017

# Safety with Technology
Seguridad con la Tecnología

**Victim Services Unit**
**5555 Airport Blvd**
**Austin, TX 78751**
**512-854-9709**

**Name/ID Number:**

**Direct Number:**

**Mailing Address:**
**PO Box 1748**
**Austin, TX 78767**

## Technología y Riesgo

No hay duda de que la tecnología moderna es asombrosa. Nos permite entretenernos constantemente, nos permite realizar las tareas que nunca pensamos fueran posibles, y nos permite estar "conectados" en todo momento. Sin embargo, toda esta conexión tiene un aspecto negativo: los riesgos de seguridad. La tecnología moderna nos deja vulnerables/desprotegidos a los riesgos de todo, desde el robo de identidad al acoso. A menudo, estos delitos afectan a aquellos que no se dieron cuenta de que la información estaba bajo riesgo.

## Navegación/Exploración Básica en la Red

**Regla # 1: Navegación segura y Verificación de 2 pasos.** Al acceder a sitios web que contengan o pueden obtener sus datos personales, usted debe asegurarse de que el prefijo/titulo a la dirección web es "https" en lugar de "http". Esto codifica la página y protege contra hackers que puedan tener acceso a ella. En la cuenta de seguridad / privacidad de la configuración, puede (y debe) elegir esta opciones para sus perfiles de Facebook y cuentas de correo. También a veces puede elegir ser notificado cada vez que un nuevo dispositivo/archivo inicia una sesión en su cuenta. Si un dispositivo/archivo no reconoce los registros en su cuenta, cambie su contraseña inmediatamente y compruebe si hay una violación.

**Regla # 2: Si usted no está seguro de dónde vino el mensaje, no haga clic en él, no lo abra o no lo descargue.** Los hackers y estafadores le enviarán correos electrónicos y publicaciones con enlaces llamativos en las páginas web que pueden infectar su correo electrónico y computadora con virus, robar su información personal, o un enlace que será una estafa. Si usted recibe un correo electrónico sospechoso o una dirección de correo electrónico de un desconocido, y su computadora lo etiqueta como "spam" bórrelo sin abrirlo. Si usted está "navegando" o explorando en la computadora y ve un enlace que usted no cree que sea seguro o no es de una fuente de confianza, mejor evítelo, no lo habrá.

**Regla # 3: Realice/ revise rutinariamente la seguridad y mantenimiento de su computadora.** Compre un programa de seguridad para escanear y limpiar su ordenador de virus, spyware y malware a diario o semanalmente. Contacte a su tienda local de computadoras para que le den sugerencias o lea los comentarios en la red. También debe eliminar regularmente su historial de "navegación", limpiar su "caché" y suprimir las "cookies" (información sobre su actividad tienda web). Puede encontrar las opciones para hacer todas estas cosas en su configuración de Internet.

## Facebook y otras Redes Sociales

**Regla # 1: Tenga cuidado con lo que publica y quiénes son sus "amigos" o con quien intercambia mensajes.** No divulgue información personal en sus "actualizaciones" de estado o mensajes que corresponden a las paredes/ muros de los demás. Algunos ejemplos: No deje su número de teléfono o la dirección en la "pared/muro" de nadie. Si está vinculado a cualquier persona que usted no quiere que sepa dónde está su paradero/o donde se encuentra - No publique su ubicación. No hable de cuestiones personales o jurídicas, o detalles sobre su trabajo, etc., No se involucre ni publique argumentos/ conversaciones.
No hay ninguna razón por la cual hacer amistad con toda persona que quiere ser su amigo en Facebook, especialmente extraños o con personas con las que tiene conflicto. No haga caso de las peticiones y mensajes de gente que no está seguro son de confianza, y periódicamente revise la lista y elimine personas con las cuales ya no habla. Lo mismo para los mensajes - borre sin necesidad de abrir todo lo que es de alguien que no conoce bien.

**Regla # 2: Haga su cuenta privada!** Para la planificación más segura y más allá de la protección de identidad, lo mejor es elegir la configuración más restrictiva / segura en cada configuración de su cuenta y perfil. Por ejemplo, asegúrese de que sólo sus amigos en una lista personalizada de amigos puedan ver todo en su perfil, incluyendo mensajes, fotos y otras actividades.

**Regla # 3: Tenga cuidado con los extraños!** Es sumamente importante ser cauteloso cuando se conoce a alguien en línea/red para hacer amistades, para encontrar pareja, o una transacción de una sola vez (como una venta o compra). No dé información personal a alguien con quien que conoció recientemente en por el internet. Si esa persona va a ir a su casa para comprarle algo, asegúrese de que usted no este solo en casa. Si usted va a una cita por primera vez, reúnase en un lugar público, como un restaurante. Si usted tiene un mal presentimiento en cualquier momento – Salga de allí!

**Regla # 4: Tenga cuidado con los enemigos!** Si usted tiene una ex-pareja (o alguien en su vida personal) que se ha convertido en un acosador o le amenaza por cualquier razón, limite o corte su relación por el internet con esa persona. Asegúrese de que no tienen acceso a su paradero a través de su cuenta o cuentas de sus amigos. Si está siendo acosado y amenazando a través de Facebook o cualquier otra tecnología, documente todos los incidentes y comuníquese con la policía.

**En general:** no hable de asuntos personales que podrían permitir a un desconocido o una persona con malas intenciones/peligrosa saber más de lo que usted desea. En caso de duda, pregúntese si le gustaría que una persona con malas intenciones/ peligrosa supiera lo que usted escribe. Si la respuesta es no, no lo publique o comparta.

**Consejos útiles:** Los empresarios también están buscando actividad en Facebook! Si usted no desea que su jefe vea alguna foto de usted…No la comparta!

## Su Información Personal

**Contraseñas:** Mantenga sus contraseñas privadas, y asegurarse de que sean complejas. Trate de utilizar siempre una combinación de letras mayúsculas y minúsculas, números y símbolos. Trate de no usar palabras reales en las contraseñas- utilice siglas mejor. Cambie sus contraseñas con regularidad, y no utilice la misma contraseña para todo.

**No almacene/guarde los documentos con información personal en su correo electrónico o en carpetas que no sean seguras en la red/ computadora.** Por ejemplo, no guarde los documentos con su número de Seguro Social, cuentas bancarias o números de tarjetas de crédito en donde un hacker podría tener acceso a ellos. Si usted proporciona esta información a través del Internet, por ejemplo para una transacción, asegúrese de que el sitio web que está utilizando es de buena reputación/segura, comienza con "https" y no guarde la información en inicio de sesión.

**RECUERDE: El Internet es para siempre.** Nada de lo que se elimina en Internet queda verdaderamente borrado. Y por lo general es la persona mala el que encuentra esa información.