CENTER FOR DOMESTIC PEACE
Working Together to End Domestic Violence

www.centerfordomesticpeace.org
Línea de apoyo bilingüe de 24 horas: 415-924-6616

END TECHNOLOGY ENABLED ABUSE

www.endtab.org

Esto fue producido con recursos proporcionados por EndTAB (Poner fin al abuso habilitado por tecnología). Para obtener más información, visite www.endtab.org

Guía de Seguridad Digital

Seguridad para cuentas en línea

Paso 1: Hacer un plan de seguridad desde un dispositivo seguro desconocido por el/la abusador/a.
Preocupación: Los pasos de planificación de seguridad podrían estar expuestos en un dispositivo comprometido.
Cómo: **Use un dispositivo o computadora de un/a amigo/a, la organización que lo/a asiste, etc**.

Paso 2: Cambie/Actualice las contraseñas de todas las cuentas (aplicaciones, banco, correo electrónico, Internet, teléfono, aplicaciones de pago, etc.) configure la autenticación de 2 factores cuando sea posible.
Preocupación: Las contraseñas comprometidas pueden proporcionar acceso no autorizado a las cuentas.
Cómo: **Use contraseñas que la otra parte no pueda adivinar, use una frase u oración.**

Paso 3: Eliminar y cerrar sesión en dispositivos que no son de confianza Es posible que los dispositivos del abusador/a aún estén conectados a las cuentas de la víctima.
Preocupación: El/a abusador/a puede monitorear o hacer cambios en las cuentas de la víctima.
Cómo: **Vaya a su configuración en sus dispositivos** (teléfonos, computadoras portátiles, etc.) y cierre sesión en los dispositivos donde el/la abusador/a tiene acceso. *CONSEJO: Los usuarios de Apple pueden cerrar sesión en varios dispositivos a la vez usando la configuración de ID de Apple. Para Google: en la configuración, en "Dispositivos de confianza", seleccione "Revocar todos"*

Paso 4: Actualizar información de contacto y preguntas de seguridad
Preocupación: El/la abusador/a puede cambiar la información de contacto de la víctima a un número de teléfono o correo electrónico que controle.
Cómo: **Verifique y actualice la información de contacto de todas las cuentas**, cambie las preguntas de seguridad para que sean al azar o cambie las respuestas para que sean incorrectas.

Imágenes íntimas no consentidas

Paso 1: Guardar la evidencia antes de eliminar cualquier cosa
Algunas formas de hacer esto:
a. Descargue los videos
b. Haga captura de pantalla de la página web, incluida la URL, la fecha y la hora
c. Guarde la página web como pdf, haga copias impresas.

Paso 2: Eliminar las búsquedas de Google
Escriba en Google: "Solicite eliminar imágenes explícitas no consentidas de la Búsqueda de Google" y haga clic en "iniciar solicitud de eliminación"
Visite: www.stopncii.org para obtener más información sobre cómo eliminar imágenes íntimas
CONSEJO: La mayoría de las compañías de redes sociales le permiten "reportar" estas imágenes porque violan las normas de la comunidad. Documente, luego informe para que la publicación pueda ser eliminada.
Si es necesario, una víctima también puede reclamar los derechos de autor sobre una imagen para eliminarla.

Paso 3: Explorar acción legal
46 Estados han criminalizado la pornografía no consentida. Aquí hay algunas opciones:
a.Reporte el crimen a la policía local
b. Considere una orden de restricción o protección (comuníquese con la agencia local de la VD o AS)

Consejos más seguros para el sexting

a. Sin caras, tatuajes, marcas de nacimiento
b. Fondo neutro

Quitar información de ubicación:
a. **iPhone:** seleccione la foto para enviar, seleccione "opciones", toque "ubicación" enviando las coordenadas adjuntas en la foto
b. **Android:** dentro de la aplicación Fotos, seleccione la imagen, toque los tres puntos en la esquina superior derecha, desplácese hacia abajo y toque los tres puntos junto a los datos de ubicación, toque Eliminar/quitar

Rastreo de ubicación (acecho digital)

Paso 1: Determinar si está siendo rastreado/a Haga una búsqueda física de bolsas, asientos de automóviles, vehículos, ropa, etc. Si escucha un pitido de un dispositivo o recibe una alerta de AirTag (solo iPhones)

Paso 2: Desactivar rastreadores (antes de desactivarlo, ¡cree un plan de seguridad!) Gire y deslice el panel posterior fuera del rastreador para quitar la batería.

Paso 3: Guardar evidencia- Tome capturas de pantalla de las alertas de seguridad recibidas. Tome fotos del lugar donde se descubrió el rastreador. Si es seguro hacerlo, conserve el dispositivo de rastreo. **Si no está desactivado, el/la abusador/a puede saber dónde lo ha llevado (con la policía, a la corte, etc.)***

Paso 4: Considerar denunciar el delito- Los rastreadores Tile y AirTag frecuentemente se pueden vincular a una persona. Póngase en contacto con su departamento de policía local para obtener más información.