www.centerfordomesticpeace.org
www.endtab.org
www.techsafety.org

# Digital Safety Card

What is digital abuse? Using tech to maintain power and control over an intimate partner.

## Account Safety

**Step 1:** Safety plan from a safe device unknown to the attacker. Concern: Safety planning steps could be exposed on a compromised device.
How: **Use a device or computer belonging to a friend, the organization assisting you, etc**

**Step 2:** Change/Update passwords to all accounts (apps, checking, email, internet, phone, payment apps, etc) set up 2 factor authentication when possible.
Concern: Compromised passwords can provide unauthorized access to accounts.
How: **Use passwords the other party can't guess, use a phrase or sentence.**

**Step 3: Remove and Sign Out of untrusted devices**
Abuser's device(s) may be still be logged in to victim's accounts. Concern: Abuser can monitor or make changes to the victim's accounts. Also, if you make changes be aware abuser can find out.
How: **Go to your settings on your devices** (phones, laptops, etc) and sign out of devices abuser has access to.
*TIP: Apple users: sign out of multiple devices at once. Go to: Apple ID settings. You may unshare your location and app access. Scroll down to "Safety Check". Click this video to see how it's done. For Google: In settings, under "Devices you trust," select "Revoke all."*

**Step 4: Update Contact info & Security Questions**
Concern: Abuser may change a victim's contact info to a phone number or email they control.
How: **Verify & update contact info for all accounts** change security questions to be random, or change answers to be incorrect.

## Non Consensual Intimate Images

**Step 1: Save the Evidence Before Deleting Anything**
a. Download the video(s).
b. Screenshot the webpage, including the url, date & time.
c. Save the webpage as a pdf, print hard copies.

**Step 2: Remove from Google Searches**
Type into Google: "Request to remove non-consensual explicit imagery from Google Search" and click "start removal request"
Visit: **www.stopncii.org** (if over 18, if under 18 visit **takeitdown.ncmec.org)** to learn more about removing intimate images
*TIP: Most social media companies let you "report" these images because they violate community guidelines. Document, then report so the post can be removed.*
*If needed, a victim can also claim copyright over an image to get it removed.*

**Step 3: Explore Legal Action**
46 States have made nonconsensual pornography a crime.
a. Report the crime to local law enforcement.
b. Consider a restraining or protective order (Contact local domestic violence or sexual assault agency for assistance).

## Safer Sexting Tips

a. No Faces, Tattoos, Birthmarks
b. Neutral Backgrounds

***Remove location Information:***

a. **iPhone:** Select photo to send, select "options",Tap "location" sending coordinates embedded in the photo
b. **Android:** Inside the Photos app, select the image, tap on the three dots in the upper right corner, Scroll down & tap on the three dots next location data, tap Remove.

## Location Tracking

**Step 1: Determine if You're Being Tracked**
Do a physical search of bags, car seats, vehicles, clothing, etc. If you hear a device beeping or get an airtag alert (iPhones only)
**Step 2: Save Evidence**- Take screenshots of security alerts received. Take photos of where the tracker was discovered. If safe to do so, keep the tracking device. **If not disabled, the abuser may know where you've taken it (Law Enforcement, Court, etc.)**
**Step 3: Disable Trackers** (before disabling, create a safety plan!) Twist and slide back panel off of tracker to remove battery.
**Step 4: Consider Reporting the Crime**-Tile & Airtag trackers can often be linked back to a person. Contact your local PD for more information.

This was produced with resources provided by EndTAB (End Technology Enabled Abuse). For more information visit www.endtab.org

www.centerfordomesticpeace.org
www.endtab.org
www.techsafety.org

# Guía de Seguridad Digital

¿Qué es el abuso digital? Es cuando los/as abusadores/as usan la tecnología para mantener el poder y el control sobre una pareja íntima.

## 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 Apple. Puede dejar de compartir su ubicación y acceso a la aplicación. Desplácese hacia abajo hasta **"Safety Check". Haga clic en este vídeo** para ver cómo se hace. 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** (si tiene más de 18 años, si tiene menos de 18 años, visite **takeitdown.ncmec.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.
a.Reporte el crimen a la policía local.
b. Considere una orden de restricción o protección (comuníquese con la agencia local de la violencia doméstica o agresión sexual)

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