Tips to discuss with Clients

OurFamilyWizard°

- 1. **Trust your instincts** If you suspect the abusive person knows too much, it is possible that your phone, computer, email, driving or other activities are being monitored.
- 2. **Plan for safety-** Navigating technology is a vital step in safety planning today. Make sure you discuss with your client's what technologies are being used such as: online dating, social media, Bluetooth, GPS, On-Star, and more.
- 3. **Change passwords-** While safety planning, change all account passwords that may disclose your client's location or activities. You must also remember to change the security questions if there is a possibility that the abusive party can answer the questions and obtain access to the account.
- 4. **Cell Phone settings-** If your client is using a smartphone, check the location services in the setting and see if the phone is giving away your location. Also turn off Bluetooth when not being used. This can prevent the abusive party from monitoring or installing malicious software on the phone.
- 5. **Consider a donated or new cell phone** If the cell phone being used is provided by the abusive party, contact your local hotline for possible phone donation locations. When making or receiving private calls or arranging escape plans, try not to use the phone provided by the abusive party as it may be monitored.
- 6. A safer computer- If an abusive party has access to your computer, he/she might be monitoring your computer activities. If possible, try to use a safer computer when you look for help, a new place to live, travel and etc. It may be safer to use the computer at the library, community center, or internet café.

- 7. Search for your name on the internet- By using popular search engines such as Google, Spokeo, Bing, and etc., it is important to see what information may be being made public about you. The fastest way to search is by adding quotations "before and after your name" followed by your state or city. This will help avoid finding irrelevant information from duplicate names. Don't forget to also view the "images" portion of the search engine to see what possible pictures may be public.
- 8. **Social Media-** Discuss the safety and privacy setting for any and all social media accounts being used. It may be important to change some of the privacy settings to ensure that your client's location is not being compromised or that harmful information is not being shared.
- 9. Ask about your records and data- Many court systems and government agencies are publishing records to the internet. Ask agencies how they protect or publish your records and request that court, government, post office, and others seal or restrict access to your files to protect your safety.
- *10.* **Consider optional phone services-** With technology, services such as "Google Voice," may be a better alternative in keeping your personal phone numbers safe. With services such as these, you can sign up for a phone number and have that number forward to up to five different phones. So that way if your phone number is compromised, you can log in and change one phone number rather than having to contact the phone companies and changing many.
- 11. **Consider Tracker Detection Apps-** Inside the App Store or Play Store you can find apps to help detect trackers such as GPS, Apple Air Tags, Tiles and more. Some of the available apps are: Tracker Detect, the Tile App, and Crowd GPS Scanner.

Steven Bradley, Safety and Technology Expert sbradley@ourfamilywizard.com 850-294-3413