

DIGITAL SAFETY PLAN

LOCATION:

For iPhone Users

* If using an iPhone turn off “Find iPhone” so your abuser cannot find you by finding out where your phone is

1. Go into the Settings app
2. Scroll down to Privacy
3. Within Privacy scroll down to Location Services
4. Slide location services OFF
5. Turn OFF when prompted

For Android users

1. Open the App Drawer and go to Settings.
2. Scroll down and tap Location.
3. Scroll down and tap Google Location Settings.
4. Tap Location Reporting and Location History, and switch the slider to off for each one.
5. To delete your phone's location cache, tap "Delete Location History" at the bottom of the screen under Location History.
6. Repeat this process for each Google Account you have on your Android device.

For Blackberry users

1. On the home screen, swipe down from the top of the screen.
2. Tap image Settings > Location Services.
3. Turn off Location Services.

CELL PHONE:

- Go to your cell phone provider and request a new phone number and to return the phone to factory settings
- Delete call history
- Keep supports / resources under a different name in your contacts; create a cover story with you support persons in case the abuser calls these numbers.
- Have phone bills sent electronically to a private e-mail address or to a friend's house

SOCIAL MEDIA PROFILE AND POSTS:

- Keep your accounts locked and private
- Use a generic name so the abuser cannot search your name to find your account
- Use a generic profile picture (i.e. a sunset)
- Do not post about where you are living/working/going to school
- Use less hashtags; hashtags make your posts more visible and easier to find
- Use less specific hashtags; do not hashtag locations, times, or events
- Do not use geo-tags (locations) on your posts
- Post after attending events and locations, rather than posting where you are at any given time
- Consider using a different city for your location on profiles

FRIENDS & FOLLOWERS:

- Change the settings so it allows you to moderate each new follower/friend who adds you
- Only add people you know and have met face to face with
- Check with the person to make sure the account adding you is actually them
- Check the profiles of the person adding you to make sure they look legitimate (pictures, posts, friends in common)
- Block/mute/delete any accounts your abuser has access to
- Block/mute/delete any accounts of users who are still connected to your abuser
- If your abuser tries to contact you, block and report the account

E-MAIL:

- Delete / deactivate e-mail accounts your abuser has access to
- Create multiple new e-mail accounts to use
- Do not use your first or last name for your new e-mail address
- Change the password on your new accounts regularly (once a month)
- Do not utilize old passwords
- Register your social media accounts with your new e-mail address
- Delete/deactivate old social media accounts

INTERNET BROWSERS

- Clear websites from your browser history that you do not want your abuser to see.
- Search in incognito mode on Google Chrome to stop websites from being added to your search bar and search history.
- Use resource websites that have an escape button so you can quickly exit out of the website if your abuser walks in
- Use public computers (i.e. at the library) to do any safety research and planning you need to do

Source: Victim Services Toronto (July 2018) available at <http://victimservicestoronto.com/wp-content/uploads/2016/06/DIGITAL-SAFETY-TIPS-IN-ABUSIVE-RELATIONSHIPS.pdf>

SMART HOME DEVICES (ALARMS, SURVEILLANCE CAMERAS, HEAT CONTROL, LIGHT CONTROL, DIGITAL LOCKS):

Smart devices allow the users to control different parts of their home using a cell phone application or remote. This can include remotely locking doors, opening a garage door, changing the heat or air conditioning, turning on or off lights, turning on music or other media.

If you have smart technology installed in your home it is important to be mindful, especially if your abuser has access to this technology. Some may use this to manipulate and control another individual, by changing passwords, turning on or off lights, turning up or down the heat, and unlocking doors after they have been locked.

- Be aware of any devices installed in your home and any video and audio recording devices in your home that can be used to monitor you
- Since smart devices can be used to record you, be mindful of conversations you have regarding safety plans in the home. Consider having safety planning conversations outside of the home.
- If you can, know passwords to the Wifi and all devices and consider changing them
- Keep reset instructions on any devices you install in your home and keep instructions on how to disable users
- Consider contacting the service provider to discontinue service and consider unplugging or disconnecting the device
- If you are receiving a criminal or family court order, ensure it includes Smart home devices.

DIGITAL SAFETY PLANNING WITH YOUR CHILDREN

- Go over the privacy and security settings of all apps before use
- Ensure their social media accounts are private and encourage them to use a generic profile picture
- Encourage them to use a nickname instead of their real name on social media
- Instruct your children to not meet up with online friends/followers
- Require all new users and friends to be approved before they see your child's profile.
- Turn off location settings on their phone and in any apps
- Encourage them not to use hashtags; these make posts more visible
- Encourage them to post after they have attended an event, when they are safe at home
- Tell your children not to post pictures in front of your home, their school, or in their school uniform and to not tag their location
- Tell your children to block and report any accounts they think might be the abuser
- Tell your children to tell you if the abuser tries to contact them

Source: Victim Services Toronto (July 2018) available at <http://victimservicestoronto.com/wp-content/uploads/2016/06/DIGITAL-SAFETY-TIPS-IN-ABUSIVE-RELATIONSHIPS.pdf>