victim services
toronto

GENERAL ONLINE SAFETY TIPS

Privacy Settings and Safety Functions

- Review Terms and Conditions, privacy setting and safety functions prior to using the website or social media application.
- Review privacy setting options & safety functions once a month to keep updated
- Review settings each time you restart your phone or download software updates

GPS/ Locator Function

Turn off the GPS tracking and locators on apps and your mobile device that reveal your location information to the public (where you are at this exact time).

For iPhone Users:

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.

If you need to use your Location Services for certain apps such as weather or maps consider turning on your location services only when the app is in use.

JULY 2018

If you are using an iPhone and will be leaving your Location Services on all the time consider turning off the significant locations settings.

For iPhone Users:

1. Go into the Settings app
2. Scroll down to Privacy
3. Within Privacy scroll down to Location Services
4. Within Location Services scroll down to Significant Locations
5. Turn OFF

Social Media

- Having a locked profile limits who can view your profile and allows you to have more control of who sees your content and who can find you through search engines and search bars.
- Change privacy setting to limit who can see your shared and tagged posts, photos, statuses, etc.
- Change privacy settings to enable you to approve tagged posts prior to being posted.
- Be aware of geo-filters and tags, they can be seen by anyone who searches that location or who can see your accounts
- Avoid adding extensions that request access to your social media accounts such as games and quizzes

Passwords

- 12 characters
- Use a mix of numbers, symbols, uppercase, and lowercase
- Change passwords often (once a month)
- Use the authenticate seal / image pop up during password reset
- Never give out your password to someone else
- Do not give out others' passwords
- Use secure networks that you trust

victim services
toronto

Online Profile

- If you use social media for your business, employment or school consider having more than one social media account; one public and one private.
- Avoid using your full name or a nickname that is easily identifiable
- Consider using a generic profile name that does not identify you at all
- Consider using a generic profile picture that does not identify you or where you live
- Avoid completing your profile description and consider leaving it blank.

Online Posts

- Be aware of the surroundings in the pictures you post. Avoid posting your school, home, neighbour's home, place of employment, or while wearing your school or work uniform.
- Avoid posting or sharing content that you wouldn't want close family members, parents/guardians, teachers, or employers to see or that you would be embarrassed for others to see
- Consider avoiding using hashtags, especially ones specific to location; the more hashtags you use the more visible your posts and profile become
- If you are using tags consider using generic tags that do not give away your location
- Avoid posting your whereabouts, daily routines and activities. If you need to post about an activity/event consider posting after the event (#latergram)
- Review your friend/follower list on a regular basis in order to know who is seeing your posts. Consider removing anyone you do not recognize or who you have not been in recent contact with.
- Ask friends and family not to tag you in posts or tag you in locations
- Avoid revealing information about your personal identity such as: your name, address, phone number, age, physical description, work/school through your profile or posts.
- Use a search engine to search your name, and your children's names once a month to verify no personal information is readily available. If information is found, contact the website directly to have the information removed.
- Verify that your phone number and home address are not readily available on online whitepages listing websites (canada411.ca, 411.ca, etc.). If they are, contact the service provider to remove your listing.

Know Your Friends & Following:

- Consider only adding individuals whom you have met face to face and have an established relationship. Avoid adding individuals whom you have never met.
    - **Stranger:** *is a person added to your list of friends on a social networking website whom you may hardly know or have never met.*
- Search the profile, posts, pictures and friends/follower lists of the person who has requested to be added to your friend/follower list to ensure the account is legitimate.
- Opt-out of 'suggested profile/friend' services from social media sites
- Look to see if you have friends in common before accepting a friend request.
- Check with the person directly before accepting a friend request to ensure that it is not a fake account.

Responding to cyberviolence

- Take a deep breath and pause; avoid retaliating.
- Continue to practice online safety habits and maintain your positive online identity.
- Take a screen capture of the comments, save private messages, texts, etc. and report to the police, a friend, parent/guardian or trusted adult
- Report the incident to the social media website and be aware that it may take several days for the social media website to respond
- Block, unfriend, or mute the individual
- Mute individual words and conversations on Twitter
- Check your privacy settings and consider locking or setting your profile to private
- After capturing the negative messages and reporting them to police consider taking your mobile device to your service provider to scan for unwanted locator apps and to return your phone to factory settings.
- Consider disabling your social media account for a brief time or deleting your account and starting a new one.
- If you are disabling your account consider changing your password and then disabling the account in case your original password was compromised.
- Reach out for support, tell a trusted friend and/or adult such as a parent/guardian, family member, teacher, social worker, principal, school resource officer or police.
-

- If you are receiving online threats, ongoing negative and mean comments, sexualized images or being contacted by someone who is asking for your personal information or for you to do things you feel uncomfortable with report it to police 416-808-222 or anonymously to crime stoppers 1-800-222-TIPS (8477)