SHAMSAHA

Stalking and Cyberstalking

What is stalking?

Stalking is any repeated, obsessive and unwanted contact with you that makes you feel afraid or unsafe. A stalker can be someone you know, a past boyfriend or girlfriend or a stranger. You can be stalked by anyone, but actually three in four victims are harassed by someone they know.

Stalking is serious and may get worse or become violent over time. Stalking may also be a sign of an abusive relationship. Stalkers may threaten your safety by clearly and directly telling you they want to harm you. Some stalkers may harass you with less threatening but still unwanted contact. Stalking which involves the Internet, email, or other electronic communications is known as "cyberstalking". Stalking can be traumatic. You may experience nightmares, lose sleep, get depressed or feel like you're no longer in control of your life.

Examples of what stalkers may do:

- Show up at your home or place of work unannounced or uninvited
- Send you unwanted messages, letters, and emails
- Leave unwanted items, gifts or flowers
- Constantly call you and hang up
- Use social networks online and technology to track you
- Spread rumors about you via the internet or word of mouth
- Make unwanted phone calls to you.
- Call your employer or professor
- Wait at places you visit
- Use other people as resources to investigate your life (such as going through your Facebook or Instagram page through someone else's user or adding your friends in order to get more information about you)
- Damage your home, car or other property
- Following you around or spying on you
- Threatening you, your family, or pets with violence

How can I respond to stalking?

- Remember to save important evidence, which includes:
  - Text messages, emails or voice messages
  - Videos
  - Letters, photos and cards
  - Unwanted items or gifts
  - Social media friend requests
- Write down important details of every incident, including the times, places, and dates
  - Include the names and contact information of people who witnessed what happened
  - If the incidents occurred online, take screenshots to maintain records
- Always have your phone with you so you can call for help
- Ask your service provider about call blocking and other safety features
- Seek out the support you deserve by telling your friends and family, employer and police about the stalking
- File a complaint with the police. Make sure to tell them about all threats and incidents
- If it is appropriate, secure your home with alarms, locks, and motion-sensitive lights
- Develop a safety plan

What is cyberstalking?

Cyberstalkers mainly rely on online technology to approach you. In the digital world, cyber stalkers are driven by the same intention – to embarrass, threaten, or harass their victims. Everything on the Internet can be used by cyberstalkers to make inappropriate contact with their victims - including email, social networks, instant messaging, personal data available online.

It is important to identify what is and is not cyberstalking. Checking out someone's social media is not online stalking. Researching a newly hired coworker's Facebook or Instagram is not stalking.

Cyberstalking involves malicious intentions, such as false accusations and defamation to sexual harassment and even encouraging others to harass the victim. In many cases, physical and digital stalking are both used to threaten the victim.

Examples of cyberstalking include:

- "Cat-fishing" which occurs on social media when online stalkers create fake user profiles and impersonate their identities as someone you know or may know.
- Monitoring your location check-ins on social media
- Hijacking your webcam

- Installing stalker-ware
- This can include any type of legitimate software or spyware that can be used to monitor someone's activities through their device. Stalk-ware is designed to run in the background without your knowledge. It can track your location, make audio recordings, and enable access to your texts and browsing history.
- Looking at geotags to track your location
- Every digital picture you take may contain geotags, which are pieces of metadata revealing where and when the photo was taken. Geotags come in the EXIF format, which is embedded into an image file and can be extracted and viewed with the help of special apps. This way, a cyberstalker can learn about your whereabouts.

Precautionary steps and how to respond to cyber-stalking:

- Send the person one clear, written warning not to contact you again|
    - If they contact you again after you've told them not to, do not respond
- Print out copies of evidence such as emails or screenshots of your phone
- Keep a record of the stalking and any contact with police
- Report the stalker to the authority in charge of the website or service where the stalker contacted you
    - For example, if someone is stalking you through Facebook, report them to Facebook
- Consider blocking messages from the harasser
- Change your email address or screen name
- Set strong and unique passwords for your online accounts and do not share them with anyone
- Google yourself to check how much information one can find about you online. If you find too much information about yourself, consider taking some of it down
- Don't open suspicious messages and don't click on unknown links or files
- Never post online profiles or messages with information that someone could use to identify or locate you (such as your age, sex, address, workplace, phone number, school, or places you hang out)

If you suspect you are being cat-fished:

- Take a look at the friends list. Cat-fishers do not usually have more than 100 friends.
- Save the profile picture and run a reverse image search on Google. If you get links to multiple profiles, it's a warning sign of an imposter.
- Review the user's photos. If there are only selfies, single-person shots or stock-style pictures, it is likely they aren't real.
- Suggest making a video call and see how the person reacts. If he or she starts making excuses, you can suspect that you're talking to a cat-fisher.

If you suspect stalker-ware on your device:

- Go to your settings or app list and look through the apps that are running in the background - make sure you recognize all of them. Delete the suspicious apps immediately.
- If you cannot delete the suspicious app or there's no app, but you still suspect something, you might need to restore your phone to factory settings. However, some stalk-ware cannot "uninstall" and you might need to get a new device.
- Check your location sharing settings for apps such as Google Maps and Find My Friends. It may be that someone has previously set up your phone to share its location with them. If so, change the settings immediately.