What is Cyberstalking

Examples of cyberstalking:

- Sending constant stream of emails or instant messages to you or your friends, family, or coworkers;
- Posting inappropriate comments or making false accusations on your social networking sites;
- Posing as you and posting inappropriate comments and personal advertisements online;
- Sending offensive emails in your name to your family, friends, significant other, boss, etc.;
- Hacking (breaking into your accounts and changing passwords or signing up for spam and inappropriate websites);
- Sending viruses to your computer (for example, spyware[1] to track your online visits as well as key strokes and other viruses meant to track or damage your computer);
- Invading your favorite sites and forums and leaving inappropriate comments or constructing inappropriate images incorporating your face;
- Creating websites that are inappropriate or questionable in your name and sending invites to your family and peers;
- Attempting to gather your personal information such as your phone number and home address that can develop into cases of offline stalking. In some cases, your personal information is posted online and soliciting sexual services or violence.
- Trying to involve third parties in the harassment by claiming that you have harmed them in some way. Posting your name and telephone number in order to encourage others to join the pursuit.
- Ordering items such as pornography or sex toys or subscribing to magazines in your name and having them delivered to your workplace.

Protection from Cyberstalking: Basic Advice

Generally, most people don’t think about cyberstalking until they are being harassed. Listed below are some basic steps individuals can take, at any time, to minimize their risk of being cyberstalked. If you have fallen victim to a cyberstalker, some of these measures will reduce the likelihood that the behavior continues.

Preventative measures* one can take:

- Choose a genderless screen name and change it if necessary;
- Create a separate email account through a free service that is not tied to personal or work addresses and is only used for online activity;
- Don't use your real name *or* nickname;

- Choose a complicated password that uses alpha and numeric characters and is of no significance. Passwords should not be shared with anyone, and a legitimate businesses will never prompt a user to give his/her password;
- Protect your privacy by not publishing or talking about your real name, address, or other contact details. Set privacy options to the most restrictive possible;
- Change online routines, so that the stalker is not able to connect easily;
- Ignore unknown communications sent to you;
- Depending on level of threat, do not confront the aggressor. If the threat level is low, send a clear message that communication is unwanted. This will act as a benchmark for any future police investigations/legal proceedings. Once it has been sent, do not respond to any further communications;
- Use filters to remove unwanted communications, and block the user from interacting with you if possible. (How to do this will vary by device, Use manual or internet search for instructions.);
- Stop using site or service (if possible);
- Do not post or give out personal information;
- Change passwords for all online points of contact, including email, IM, and social networks. If there is a risk that personal devices have been compromised, these changes should be made at a neutral site, such as a library;
- Don't have personal conversations in publicly-viewable forums;
- Refrain from publicizing any plans (personal, vacation, travel, etc);
- Learn cyber etiquette (lingo, profile rules, etc.) particular to the site being accessed;
- You can Google yourself to ensure no information is posted about you;
- If a situation becomes hostile, log off and surf elsewhere;
- Keep a handwritten log of contacts from the cyberstalker, especially if there is a possibility that the computer/device has been compromised;
- DO NOT delete original messages. Save all harassing/unwanted messages, in soft and hard copy. This will be useful if reporting to authorities;
- Take screenshots of any harassing behaviors, especially those that are hard to log like video chats. (How to do this will vary by device. Use manual or internet search for instructions.)

For more persistent harassment or escalating of the stalking behaviors or threats, or if the cyberstalking moves from the online world to direct, in person contact, please consult the fact sheet entitled “Reporting cyberstalking to the authorities.”

These suggestions assume that there is no imminent danger of physical harm. If there is such a threat, the victim must attend to their personal safety by contacting the police, family, friends, and other appropriate supports.