Cyberstalking

How to stay safe and protect yourself online

What is cyberstalking?

Cyberstalking includes (repeatedly) sending threats or false accusations via email or mobile phone, making threatening or false posts on websites, stealing a person's identity or data or spying and monitoring a person's computer and internet use. Sometimes the threats can escalate into physical spaces.

There are just as many predators on the internet as there are in real life. Anyone can be stalked online but the majority of victims as in life offline are female. Stalking estimates show that 80% of stalking victims are women[1].

And the perpetrators are not just strangers. They can also be former, estranged or current partners, boyfriends or husbands. Domestic violence victims are one of the most vulnerable groups to traditional stalking so it's no surprise they are vulnerable to cyberstalking as well[2].

As in other types of violence against women, cyberstalking is about power relations, intimidation and establishing control. If you are being stalked, know first and foremost that you did NOT "provoke" this harassment.

Who we are: APC and APC women's programme

Founded in 1990, Association for Progressive Communications (APC) is an international network and non-profit organisation that wants everyone to have access to a free and open internet to improve our lives and create a more just world. The APC WNSP is a global network of women who support women networking for women's empowerment through the use of ICTs and is a programme of APC.

www.apc.org ***www.apcwomen.org***

1 Wired Safety http://www.wiredsafety.org/cyberstalking_harassment/context.html

2 Alexis A. Moore "Cyberstalking and Women - Facts and Statistics" About.com 8 January 2009 http://womensissues.about.com/od/violenceagainstwomen/a/CyberstalkingFS.htm

How can I prevent someone from stalking me online?

• **Be careful what personal information you share online** including in email, on social networking sites like Facebook and Twitter and chat rooms. It is very easy to glean information about where you live, the places you love to go to in your area and the people you care about from posts and pictures.

• **Create a different email account for registering in social networking sites** and other online spaces. It will help avoid spam and your personal email won´t be revealed if the online service doesn't have a good privacy practice.

• **Do not feel obligated to fill out all fields when registering online** or provide identifying information such as birthdates and place in required fields.

• **In your online user profile, use a photo that doesn't identify you** or your location, so you can't be recognised.

• **Consider using a name that is not your real name** or a nickname as your email name, screen name or user ID. And try not to use common dates such as your birthday as the digits in your email name or password. Instead, pick a name that is gender- and age-neutral. Treat your email and/or internet account like you would your credit card, ID or passport number – very carefully.

• **If you are breaking up with an intimate partner** – especially if they are abusive, troubled, angry or difficult – **reset every single password on all of your accounts**, from email and social networking accounts to bank accounts, to something they cannot guess.

• **Services such as Facebook change their privacy policy all the time, so it is a good idea to check your privacy settings** to make sure you are sharing the information you want to share with people you trust and not the general internet public. Some sites have options for you to test how your profile is being viewed by others – test and make sure you only reveal what is absolutely necessary.

• **What information are family and friends posting about you?** Let them know your concerns about privacy and help them learn better privacy settings.

• **Do an internet search of your name regularly** and monitor where you appear online. If you find unauthorised info about yourself online, contact the website moderator to request its removal.

• **Make sure that your internet service provider (ISP), cell phone service, instant messenger** (called internet relay chat, or IRC in some terms of service) **network and other services you use has an acceptable privacy policy that prohibits cyberstalking.** If they have none, suggest they create one and/or switch to a provider that is more responsive to user privacy concerns and complaints.

• **If you have a blog or personal website you maintain,** please read the information on the next page.

What should I do if someone starts stalking me online?

• **Trust your instincts.** If you feel uncomfortable or an online situation becomes hostile, remove yourself from the online space by logging off or surfing elsewhere, or block the other person´s access to you.

• **If you are receiving unwanted contact, make clear to that person that you would like him or her not to contact you again.** Many women who have reported being harrassed do this and warn that any further contact will result in the filing of a police report. Depending on the harasser, engagement with the person can escalate or cease, so if you consider contact appropriate and necessary, do so once and document it.

• **Save all communications with the stalker for evidence.** Do not edit or alter them in any way. Try using print screens, especially if the harrassment is happening in real-time.

• **If the harasser posts comments on your blog, keep copies** but also consider unpublishing rather than deleting abusive posts.

• **Keep a record of your communications with internet system administrators or law enforcement officials** if you report the stalker to authorities. Record-keeping is absolutely crucial so keep everything, even though the immediate desire might be to delete the communication from the stalker and try to forget about it. Back up these communications on another computer or removable memory stick or external hard drive.

• **Consider blocking or filtering messages from the harasser.** Many email programs have a filter feature. Chat room contact can also be blocked, and you can activate the 'IP address block' option on your blog or website if someone posts harassing comments continuously.

• **If your internet searches reveal that the stalker is publishing harmful information about you in other online spaces, make a complaint to the moderators/managers of the external site.** State that you view this as part of a continuing situation of online harassment towards you, and request that they either block the harrasser's IP, remove posts, or caution the harrasser to cease or be blocked.

• **Tell your family and friends that someone is stalking you online.** Being stalked – online or offline – is a traumatic experience and support from your family and friends is critical at this time to help you cope. Also check what they are revealing about you and their relationship with you in their online spaces, albeit inadvertently.

• **Tell your employer that someone is stalking you** if you think this person may harass you in the workplace. Your employer will be more likely to back you up if they receive harassing or questionable messages about you from the cyberstalker, and they may be helpful in mitigating any professional damage.

This person won't stop harassing me and I want to report the abuse. Where do I file a complaint?

• **If harassment continues after you have asked the person to stop and/or the harassment escalates, contact the harasser's internet service provider.** Most ISPs have clear policies prohibiting the use of their services to abuse another person. Often, an ISP can try to stop the conduct by direct contact with the stalker or by closing their account. If you receive abusive emails, identify the domain (after the "@" sign) and contact that ISP. Most ISPs have an email address such as abuse@domain name> or postmaster@domain name> that can be used for complaints. If the ISP has a website, visit it for information on how to file a complaint. Follow up with the ISP and make sure action is being taken, and keep all communications with the ISP.

• **Check with your own ISP to assist in blocking a stalker's access to you** and consider changing services if they are insensitive to your requests or have no policies.

• **Check out which bodies or agencies are available in your country and community that can investigate and take action in online harassment cases.** Contact the police or other relevant agency and inform them of the situation in as much detail as possible, providing copies of your documentation of the harrassment.

• **Remember to keep all communications with police as a record of evidence** as well. Depending on your country, harrassment and stalking may not be typified as a crime, or local police may not be aware of recent applications of harassment law to cyberstalking. If you are not finding local recourse, consider appealing to national cyber-police mechanisms and/or women's safety advocates. If you are having trouble contacting the right body, write to help@takebackthetech.net. We'll see if we can point you in the right direction.

I'm a blogger. How can I protect myself?

• **Don't post your email address.** Instead, create a simple contact form where the person can post and submit THEIR information in order to get in contact with you.

• **Require that people sign up for an account in order to post comments** or activate the option to track IP addresses of commenters (to find out more about IP addresses and tracking them, go to: http://wikihow.com/Trace-an-IP-Address).

• **Subject all comments to prior approval** before they are posted publicly, or merely publish your policy for acceptable posting (for example, take a look at the comments policy for the feminist blog Feministing http://feministing.com/about/ to get an idea of what yours could be like). Do check your comments regularly and delete those that surpass the boundaries of your established criteria.

• **Did you know that when you register a domain name (the website's name), your contact information – name, address, phone number and email – is made public and available for anyone to see?** This is a transparency requirement in many countries. While domain proxy services exist for a fee to protect privacy, even these have proven unreliable in the face of legal or public pressure to reveal registry information. So, if you have your own website domain, you might use an organisational address and phone number, or one that does not reveal your home location. Create an email account exclusively for managing the domain.