Fact Sheets: Cyberstalking

For kids:

What is cyberstalking?

Stalking is a process that some people use to scare, threaten or control someone else by following them and keeping track of their movements. It doesn't happen just once – it's repetitive and aims to make the victim feel unsafe. Being stalked is scary and can cause a lot of emotional hurt. Sometimes a stalker might progress to hurting a target physically, too. Cyberstalking is basically the same thing, using the Internet. A cyberstalker might:

- **Use emails to threaten you and their family and friends**
- **Find a way to get into your social media accounts (hacking), where they'll post offensive comments**
- **Create fake social media profiles, nasty websites or blogs about you**
- **Get hold of your personal emails, photos and texts to hurt you**
- **Sharing your name, address, phone number and other personal details with others to harm you**
- **Use information from the Internet to harass or blackmail you**
- **Post real or fake rude photos of you or members of your family**
- **Track your movements and daily habits so they can harass or hurt you face-to-face or steal from your house when it's empty**

Fortunately, there are a few simple ways to help keep cyberstalkers out of your life. The most important is to *always* tell your parents, a teacher or other trusted adult about what's happening so they can help you solve the problem. You can also:

- **Make sure your parents have installed good antivirus software on your devices**
- **Ask your parents if they've installed a VPN on your devices (this helps protect your personal information online)**
- **Make it tougher for cyberstalkers by using good, hard-to-guess passwords on all your online accounts**
- **Ask your parents to explain what 'phishing emails' are and how you can avoid them**
- **Be really careful what you upload to social media – the more personal information you provide, the easier it is for cyberstalkers and other online bullies to hurt you**
- **Don't post a lot of photos on social media that show where (and when) you like to hang out – cyberstalkers can use this information to harm you in some way**

For teens:

The different faces of cyberstalking

Cyberstalking is a form of online bullying taken to the extreme. It's a persistent, malicious type of harassment where a target is stalked using the Internet. Individual motivations can vary but generally, an online stalker's aim is to control, intimidate or influence their target or damage their reputation.

A cyberstalker can be someone you've known for years or someone you just met online an hour ago. They strive to make you feel terrible about yourself or scared and they can do this in all sorts of ways: by slandering you, making false accusations against you, soliciting you for sex, stealing your identity, collecting personal details about you which they use to harass, embarrass or threaten you, etc. Online stalking can sometimes carry over into the offline world. Either way, it can cause a lot of pain to its victims - emotionally, financially, socially and health-wise.

Here are just some of the methods a cyberstalker might use to harass you:

- **Make up lies and spread rumours on social media to sully your reputation or attack your social status**
- **Harass your family members to make you feel even more isolated**
- **Weasel their way into your social circle to gather personal info they can use against you**
- **Steal your identity and then engage in harmful activities under your name – this can involve anything from putting viruses on your computer to hacking your online accounts to steal from you**

Cyberstalking can involve sharing of intimate photos or messages, homophobic slurs, blackmail, revenge porn, threats to expose private information and much more. It's not uncommon for this kind of stalking to involve past or present intimate partners, who use online harassment to social isolate their targets or punish them for perceived injustices.

If you become involved in a cyberstalking situation, get help as soon as possible for your own well-being and safety:

- **Report the abuse to the relevant social platform**
- **Protect your online activities with an antivirus program and VPN**
- **Take screenshots of any offensive messages or images you receive online, in case the perpetrator deletes the material later**
- **Report the abuse to your teachers, parents or other responsible adults**
- **Many forms of online abuse are illegal so don't hesitate to involve the police if you feel it's warranted**

If cyberstalking becomes a problem for you, don't let it get worse – talk to someone!

For parents

How to prevent cyberstalking and protect your kids

As adults, most of us have a pretty good idea of just how dangerous the Internet can be. Malware, viruses, identity theft, cyberbullying and an array of online scams are all out there waiting to inflict pain on the unwary – but in many ways, digital connectivity is more dangerous for our kids, who may not fully understand the risks. Cyberstalkers use a variety of methods to harass, threaten, intimidate or try to control your children. They may be schoolmates wanting to exert power, spurned boyfriends or girlfriends who won't take no for an answer, sexual predators trying to gain your child's confidence (online grooming), identity thieves or simply cyberbullies who have ramped up the abuse to 'full stalking level'. They might even infiltrate your child's social media posts to learn about upcoming holiday plans so they can burglarise your house.

Cyberstalking involving children can be extremely serious but there are ways to reduce the risk. Here are some good first steps:

- **Talk to your kids – open communication can mean the difference between your child confidently asking for your help with online issues or hiding things from you**
- **Understand the mind of a cyberstalker – quite often, they and your child may already have an in-person relationship and that interaction moves online because of social disapproval or illegality**
- **Make sure you have access to your kids' devices - this is about their protection, not their privacy; how often you use that access depends on your child and your levels of trust and concern, but kids should know that you may occasionally check up on their online activities for their own safety**
- **Invest in a high-quality antivirus program for all your child's devices to protect them from malware; think about using a VPN (Virtual Private Network) which can boost online safety, especially in public Wi-Fi areas**
- **Have a serious talk with your child or teen about what's safe and appropriate to post online and what's not (images, texts and personal information)**
- **Ensure children understand how to use the privacy settings on their devices to control who sees what; show them how to block unwanted messages**
- **Collect evidence – save emails, take screenshots, etc.**
- **Report cyberstalking to the police or children's services, the child's school and/or online and phone providers as applicable**