Cybervictimization: Cyberbullying, Cyberstalking, Online Harassment

What Is Cyberstalking?

Cyberstalking is the use of information technology to intentionally and repeatedly harass, threaten, and intimidate a specific victim. Some of the methods used to cyberstalk include e-mail, instant messaging, text messaging, or other electronic communications. It is similar to “traditional” stalking but the use of technology renders the perpetrator anonymous. A cyberstalker intends to cause fear or harm. Cyberstalking is serious and can escalate over time.

Examples of Cyberstalking (including but not limited to):

• Sending messages that threaten to harm you or your loved ones.

• Monitoring your profile(s) on social networks such as Facebook, MySpace, Twitter, etc.

• Spreading rumors about you using electronic communications.

• Compromising your on-line profiles or forging false or demeaning profiles on social networking sites.

• Posting or sending to you threatening pictures or images.

• Monitoring your phone use or repeated calling and hang-ups.

What To Do if you are Being Cyberstalked

• If you are in immediate danger, call
  • 911, or
  • Department of Public Safety on campus:
    • #3333 (from any Verizon, ATT, Spring/Nextel or T-Mobile cell phone)
    • 301-405-3555 from any off-campus phone

• If you think you are being cyberstalked, move fast! Many victims do not believe at first that it is happening to them so they do not take action. The quicker you are to block their ability to cyberstalk you, the quicker they will lose interest.

• Communicate a one-time message to the stalker to stop the behavior such as, “I do not want to hear from you. Do not contact me again.”

• If the unwanted communication is occurring in an instant messaging or chat system, log off and stay off line for 24 hours.

• Keep evidence of being cyberstalked. This means copies of emails, IMs, texts, phone messages, etc.

• Document every incident of the stalking. Write down the time, date and place of the cyberstalking occurrence. You might even consider keeping a journal to record cyberstalking activity.

• Report the cyberstalking to the Public Safety/University Police, Project NETHics, and (if the stalker is known) the Office of Student Conduct.

Tips to Protect Yourself

• Do not share any account password with anybody. Make sure all your accounts are password protected. Make sure these passwords are complex and your “security” questions are not known by others.

• If you are breaking up with a partner, change every single password on all of your accounts to something that he or she could not guess. You may also want to get a new cell phone and/or a credit card account that your partner is not aware of.

• Do not respond to unwanted messages or engage in exchanges with people that you do not know.

• Select conservative privacy settings on social networking sites (for example, limit who can see your content and posted pictures, etc.).

Selected Information from “How to Help a Friend or Partner”

What do victims need from their friends?

• Let them feel whatever it is they are feeling. Your friend may be angry, sad, frustrated, scared — or anything else — and those feelings may change every day — or every hour. It is not your job to tell your friend what they should be feeling but to accept whatever they are feeling at that time.

• Sit with them when they are having a bad day or night. You just being around may be what your friend needs. Do not assume that you need to talk or act to make an impact. Follow your friend’s lead in determining what they need and, if you don’t know what they need or want, ask.

• Your friend needs to remain in control of her/his decisions. If your friend asks you what to do, give options and let them make their own decisions.

• Understand that your friend will go through many phases in their healing process. At some points, your friend may appear to be “back to normal.” Do not assume that your friend is healed. Tomorrow may be a very different kind of day.

• Control your own shock, guilt, and anger about the situation. You have the right to your feelings about what happened to your friend but that is an issue that you are responsible for handling, perhaps by getting help for yourself. It is not your friend’s job to help you deal with their victimization.

See more at: www.health.umd.edu/node/200

Resources and References

For information on external resources, and for sources of information used to prepare this brochure, please see: www.nethics.umd.edu/resources/cybervictimization
How Project NEThics Can Help

Project NEThics is a group within the Office of Information Technology Security unit charged with promoting the acceptable use of information technology and investigating incidents of computing resources misuse. We enforce the Policy on the Acceptable Use of Information Technology Resources (www.umd.edu/aup). We are staffed with personnel equipped to handle sensitive issues, beyond technical concerns. Project NEThics can:

- Examine email messages to attempt to identify the point of origin.
- Examine logs that reflect account accesses.
- Collaborate with law enforcement to pursue case investigation.
- Identify appropriate resources to assist the victim.
- Support the victim by appearing at university hearings to provide testimony on the evidence.
- Staying in contact with the victim throughout the process by notifying her/him of our progress and answering questions that may arise.

Additional Resources

Although Project NEThics is especially equipped to handle issues of information technology, we often work with other campus resources who can provide counsel, assistance and advice.

- **Department of Public Safety** on campus: #3333 (from any Verizon, ATT, Spring/Nextel or T-Mobile cell phone); 301-405-3555 from any off-campus phone
- **Project NEThics**: 301-405-8787
- **Sexual Assault Response and Prevention Program and Advocate Office**: 301-314-2222; sarppadvocate@health.umd.edu; AIM: UMSARPPAdvocate
- **University Health Center and Faculty Staff Assistance Program**: 301-314-8180
- **Counseling Center**: 301-314-7651
- **Campus Compliance Officer**, Office of Diversity and Inclusion: 301-405-2839
- **Office of Student Conduct**: 301-314-8204
- **Resident Life Rights and Responsibilities**: 301.314.7598
- **Undergraduate Student Legal Aid**: 301-314-7756
- **Graduate Student Legal Aid**: 301-405-5807

---

**Protect Your IT Shell**
Cyberstalking • Cyberbullying • Online Harassment

---

**Project NEThics**
Office of Information Technology

4413 Computer & Space Sciences Bldg.
University of Maryland
College Park, Maryland 20742

**Phone**: 301.405.8787
**Fax**: 301.405.0720
**E-mail**: nethics@umd.edu

Revised August 2011