



Monthly Security Tips

NEWSLETTER

Department of Accounting and General Services
Information & Communications Services Division

January 2007

Volume 1, Issue 8

Dealing with Cyberbullies

Though MS-ISAC Tips often relate to workplace cyber security, Cyberbullying, or harassment through electronic messaging, can affect adults at work or at home, but it is more common for youth to be exposed to this dangerous behavior. Cyberbullying can occur via cell phone text messaging, email, instant messaging, or even within online games and social networking sites. The threats, rumors, abuse, and lies that are often used in cyberbullying are not only difficult to escape, they can also have long lasting, detrimental effects on children.

In an effort to educate our citizens and protect our youth from this growing trend, the MS-ISAC offers this tip from US-CERT on how to identify and protect yourself and your children from cyberbullies. In addition, there are also useful resources and guides included at the end of this Newsletter. Please feel free to share this with your family and friends.

Bullies are now taking advantage of technology to intimidate and harass their victims. Dealing with cyberbullying can be difficult, but there are steps you can take.

What is cyberbullying?

Cyberbullying refers to the new, and growing, practice of using technology to harass, or bully, someone else. Bullies used to be restricted to methods such as physical intimidation, postal mail, or the telephone. Now, developments in electronic media offer forums such as email, instant messaging, web pages, and digital photos to add to the arsenal. Computers, cell phones, and PDAs are new tools that can be applied to an old practice.

Forms of cyberbullying can range in severity from cruel or embarrassing rumors to threats, harassment, or stalking. It can affect any age group; however, teenagers and young adults are common victims, and cyberbullying is a growing problem in schools.

Why has cyberbullying become such a problem?

The relative anonymity of the internet is appealing for bullies because it enhances the intimidation and makes tracing the activity more difficult. Some bullies also find it easier to be more vicious because there is no personal contact. Unfortunately, the internet and email can also increase the visibility of the activity. Information or pictures posted online or forwarded in mass emails can reach a larger audience faster than more traditional methods, causing more damage to the victims. And because of the amount of personal information available online, bullies may be able to arbitrarily choose their victims.

Cyberbullying may also indicate a tendency toward more serious behavior. While bullying has always been an unfortunate reality, most bullies grow out of it. Cyberbullying has not existed long enough to have solid research, but there is evidence that it may be an early warning for more violent behavior.

How can you protect yourself?

- **Be careful where you post personal information** - By limiting the number of people who have access to your contact information or details about your interests, habits, or employment, you reduce your exposure to bullies that you do not know. This may limit your risk of becoming a victim and may make it easier to identify the bully if you are victimized.
- **Avoid escalating the situation** - Responding with hostility is likely to provoke a bully and escalate the situation. Depending on the circumstances, consider ignoring the issue. Often, bullies thrive on the reaction of their victims. Other options include subtle actions. For example, if you are receiving unwanted email messages, consider changing your email address. If the bully does not have access to the new address, the problem may stop. If you continue to get messages at your new account, you may have a stronger case for legal action.
- **Document the activity** - Keep a record of any online activity (emails, web pages, instant messages, etc.), including relevant dates and times. In addition to archiving an electronic version, consider printing a copy.
- **Report cyberbullying to the appropriate authorities** - If you are being harassed or threatened, report the activity to the local authorities. Law enforcement agencies have different policies, but your local police department or FBI branch are good starting points. Unfortunately, there is a distinction between free speech and punishable offenses, but the legal implications should be decided by the law enforcement officials and the prosecutors. Depending on the activity, it may also be appropriate to report it to school officials who may have separate policies for dealing with activity that involves students.

Protect your children by teaching them good online habits (see [Keeping Children Safe Online](#) for more information). Keep lines of communication open with your children so that they feel comfortable telling you if they are being victimized online. Reduce their risk of becoming cyberbullies by setting guidelines for and monitoring their use of the internet and other electronic media (cell phones, PDAs, etc.).

Copyright Carnegie Mellon University, Produced by US-CERT
www.us-cert.gov/cas/tips/ST06-005.html

The following sites offer additional guidance for protecting you and your children from cyberbullies:

The Internet Keep Safe Coalition <http://www.ikeepsafe.org/>

McGruff.org www.mcgruff.org/advice/cyberbullies.php

“Power In You” www.powerinyou.org/?id=Mz12

Microsoft www.microsoft.com/athome/security/children/griefers.msp

USA Today and StaySafeOnline <http://www.usatoday.com/educate/cybersecurity/20060927-cyber4-bullying.pdf>

Brought to you by:

 <p>Information & Communications Services Division (ICSD) Cyber Security Team www.cybersecurity.hawaii.gov</p> <p>The mission of the ICSD Cyber Security Team is to preserve the confidentiality, integrity, and availability of the State of Hawaii’s electronic information resources.</p>	 <p>Multi-State Information Sharing & Analysis Center www.msisac.org</p> <p>The mission of MS-ISAC is to provide a common mechanism for raising cyber security readiness and response in each state and with local government.</p>
---	--

The information provided in the Monthly Security Tips Newsletters is intended to increase your security awareness and to help improve the organization’s overall cyber security posture.