



**Cyber-bullying: A Digital Epidemic**  
White Paper

## What is Cyber-bullying?

The past two decades have witnessed a virtual explosion in new technology that has been eagerly embraced by adolescents worldwide. New technology has many social and educational benefits, but caregivers and educators have expressed concern about the dangers young people can be exposed to through these technologies. While the benefits of new technologies outweigh the costs, the anonymity that the Internet allows has given rise to a new form of peer-to-peer harassment called cyber-bullying. As kids today spend more time online, texting, watching television, and playing video games than they do with their families or in school, acts of online aggression may have greater impact than many adults realize.

Cyber-bullying has become a recently recognized, but real, problem and is defined by the Centers for Disease Control as “any type of harassment or bullying (teasing, telling lies, making fun of someone, making rude or mean comments, spreading rumors, or making threatening or aggressive comments) that occurs through email, a chat room, instant messaging, a web site (including blogs), or text messaging.”<sup>1</sup>

Acts of cyber-bullying include:

- Creating fake social media profiles on MySpace or Facebook
- Sending unwanted and insulting email and instant messages
- Hurtful Internet polling (Who’s hot, who’s not?)
- Stealing passwords
- Posting embarrassing or harmful images online
- Posting personal information including real name, address and telephone numbers online

This list is by no means complete and, in reality, the only limit to cyber-bullying is the imagination of the adolescent inflicting the abuse. And while cyber-bullying bears similarities to the traditional definition of bullying, new aspects make it even more insidious: online anonymity makes it easier for bullies to inflict damage without worrying about consequences; hurtful comments and embarrassing pictures spread quickly on the Internet; bullying spreads from an online environment to all aspects of the victim’s life; and because it occurs online it can be particularly damaging, and teachers and parents have a harder time detecting it. Also, kids may hesitate to tell adults what happens online because they are traumatized, fear retribution, or worry that their online activities might be restricted. Cyber-bullying opens the door to 24-hour harassment. Children can no longer get away.

---

<sup>1</sup>Hertz MF, David-Ferdon C. Electronic Media and Youth Violence: A CDC Issue Brief for Educators and Caregivers. Atlanta (GA): Centers for Disease Control; 2008. [http://www.cdc.gov/ncipc/dvp/YVP/electronic\\_aggression.htm](http://www.cdc.gov/ncipc/dvp/YVP/electronic_aggression.htm)

According to Harold Nieberg, "In the old days kids would threaten to beat someone up, but now it's gone into the cyberworld. Kids go onto Facebook because they get a wider audience than in the hallway."<sup>2</sup>

### How Kids Connect Today

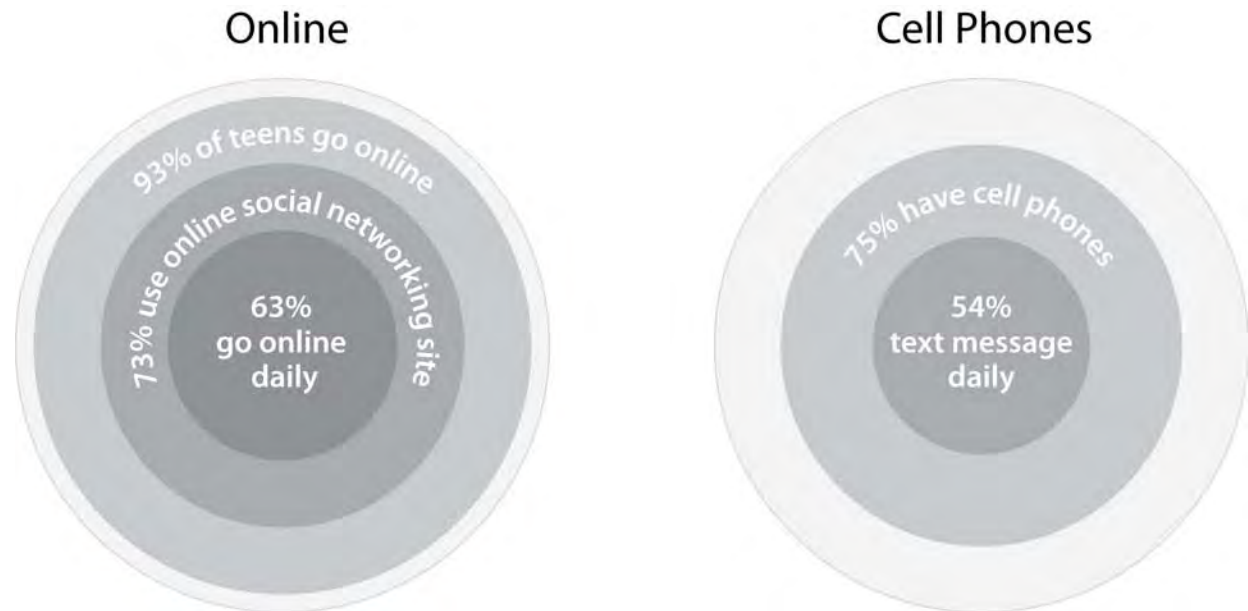


Figure 1. Online and cell phone behavior of teens (Source: Lenhart A. Cyber-bullying 2010: What the Research Tells Us)

One in three kids say that they've experienced some form of online harassment.<sup>3</sup> Of those, 30 percent experienced bullying via social networking sites, 29 percent playing online games, and 40 percent via instant messenger. With the number of victims on the rise it's important to understand the effects of cyber-bullying. Studies show extremely troubling statistics and indicate that the epidemic may have long-term and extremely damaging results such as:

- Victims of online harassment were significantly more likely to use alcohol or other drugs, receive school detention or suspension, skip school, or experience emotional distress than those who were not harassed.<sup>4</sup>
- Kids who receive rude or nasty comments online are significantly more likely to report feeling unsafe at school.<sup>5</sup>
- Targets of cyber-bullying were eight times more likely than all other youths to carry a weapon to school.<sup>6</sup>

<sup>2</sup> YUNJI DE NIES, SUSAN DONALDSON JAMES and SARAH NETTE, ABC News, <http://abcnews.go.com/Health/cyber-bullying-factor-suicide-massachusetts-teen-irish-immigrant/story?id=9660938&page=2>

<sup>3</sup> Harris Interactive/McAfee (2010)

<sup>4</sup> Ybarra M, Diener-West M, Leaf PJ. Examining the overlap in Internet harassment and school bullying: implications or school intervention. *J Adolesc Health* 2007;41(6 Suppl 1):S42-S50.

<sup>5</sup> Ybarra M, et al (2007).

Almost as troubling as the impact of cyber-bullying is the limited understanding of how we prevent it.

WatchGuard understands the explosive cyber-bullying challenge facing educational institutions as young people continue to embrace the Internet. WatchGuard education solutions provide a level of security and flexibility that allows schools to offer Internet access and network connectivity in a safe and controlled environment, while protecting students and their data. With WatchGuard education solutions individual schools and districts can efficiently and comprehensively implement a wide-ranging network security strategy to keep students safe.

### **WatchGuard XCS Stops Cyber-bullying before it Starts**

Kids are constantly connected, not only at home, but also at school. With the increased use of social networking sites, such as Facebook, and the increased likelihood and easy access to electronic tools, school IT departments now need ways to prevent cyber-bullying. Also, with increasing legislations putting the onus on school officials to protect the safety and privacy of their students and staff, some schools are simply blocking student access to these messaging media. However, with the wealth of knowledge available to students on the Internet, this could prove to be counterproductive to the learning process.

On the flip side, rather than blocking access to valuable Internet and email as educational tools, other schools are turning to email and web security solutions to help in their battle against cyber-bullying. However, most web and email security solutions focus only on in-bound content to protect the internal environment and do not focus on what is going out. With the advancement in network security technology, there are ways to fight cyber-bullying before it escalates.

As the messaging landscape continues to expand beyond just email to include messaging across web protocols and applications, it is more important than ever to have a unified solution to block threats, and holistic visibility to monitor and control content from a single point of administration. Just the thought of monitoring and controlling content across email, web, social networks, and the host of Internet tools used by the digital generation can be daunting. Where does a school start, and how can it provide effective protection with a limited budget?

The WatchGuard XCS is unique in that it provides the ability to monitor and block malicious or slanderous messaging across email and web in a single solution. By monitoring all inbound and outbound communications with a solution that intelligently finds the threats, categorizes them, and takes the appropriate remediation action defined by the school or district policies, school districts can take decisive action against cyber-bullying.

WatchGuard XCS extends email and web protection beyond anti-spam, anti-malware, and URL filtering with the integrated ability to scan all inbound and outbound content and attachments using granular content controls, such as objectionable content filtering. By monitoring and blocking malicious messages from reaching their intended recipients, schools can stop cyber-bullying in its tracks. Potentially malicious, hurtful, or slanderous messages can be blocked, quarantined, and logged, and

---

<sup>6</sup> Ybarra M, et al (2007).

alerts or copies sent automatically to principals, counselors, or relevant authorities, so they can act quickly and proactively.

### **Enforcing the Rules with WatchGuard XCS products**

- **Define and enforce acceptable use and objectionable content control policies for email and web**
  - When students send an email that contains slanderous, harmful, or potentially objectionable content, the message can be blocked, quarantined, or rerouted. At the same time, email notifications can be issued to the sender or to an appropriate authority figure as defined by the school's policy. In addition, web pages or inappropriate web postings can be blocked.
- **Control access to web sites and limit usage for learning enablement**
  - Restricting access to inappropriate or offensive web sites while still maintaining the use of the Internet as an effective educational resource is the goal of most school acceptable use policies. An example is YouTube. Quite often used as a teaching resource in schools, YouTube can also be the vehicle for cyber-bullying. The ability to block access to the site or uploads for students, while allowing teachers full access, is essential for a balanced policy.
- **Monitor email usage**
  - XCS provides the ability to monitor SMTP and webmail traffic. Abusive, threatening, offensive or simply hurtful emails are easy to control and monitor.
- **Issue notifications of inappropriate or threatening communications**
  - Notifications can be used to inform and educate students that they have sent messages that violate policies. In addition, because messages can be blocked bi-directionally (inbound and outbound), XCS prevents the intended recipient from receiving the malicious message or prevents inappropriate, slanderous content about a student from being disseminated. Further, quarantined messages can be logged and offloaded for archiving and kept to form the basis of any investigation into allegations of bullying or harassment.
- **Block offensive or inappropriate content from being uploaded or downloaded**
  - Cyber-bullying is typically delivered in the form of an email, a web posting, or an entry in a blog. The ability to block emails or access to web sites containing this content is paramount to prevention. WatchGuard XCS makes it possible to block inappropriate content, including attachments, from being posted or sent in the first place; and it can alert an administrator when any student attempts to do so.
- **Use reports for holistic visibility into cyber-bullying actions and policy violations**
  - WatchGuard XCS provides consolidated reporting to assist school officials in understanding trends in email and Internet usage and possible abuse. This information is critical for the enforcement and adoption of acceptable use policies. By nature, technically savvy students will always try to find ways to circumvent the system and share the loophole with the rest of the student body. By having holistic visibility across email and web with XCS, schools have the ability to identify gaps through which students may be trying to bypass system measures for malicious or threatening communications. For example, a combination of reports may

identify one user as a serial email and Internet abuser or bully and lead to a more in-depth investigation. XCS reports provide a consolidated view of policy breaches that can also be used to help back up or repudiate any complaints or allegations of cyber-bullying or inappropriate usage of email or web. And because reports help identify trends, they provide the data schools require to continually tweak policies to keep pace with new tactics deployed by students to deliver harmful content.

This type of intelligent monitoring and content control effectively acts as a digital playground monitor, constantly searching for threatening or harmful email or web communications, and providing a proactive approach to protect students and the school from this ever-growing trend. WatchGuard XCS is an affordable, effective solution that provides the flexibility to support distinctly different policy requirements to secure student use and yet still enable staff greater freedom to do their jobs.



advanced  
network  
systems

For More Information,  
Contact Us:

800.639.6757  
[sales@getadvanced.net](mailto:sales@getadvanced.net)

[www.getadvanced.net](http://www.getadvanced.net)

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features, or functionality will be provided on an if and when available basis. ©2011 WatchGuard Technologies, Inc. All rights reserved. WatchGuard and the WatchGuard Logo are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part.No. WGCE66732\_032811