

Whitepaper on Cyberbullying in Schools & the Workplace

Abstract

This short paper intends to offer an explanation of what cyberbullying is and provide some advice on using technology to help prevent or reduce its occurrence in schools or in the workplace.

Introduction:

Over the last decade, advances in software technology and the increased availability of computer hardware & broadband connections at affordable prices have changed the way we use the Internet. It is no longer principally the domain of the corporate Marketing department, the government or academia. With the advent of what has become known as Web 2.0, there has been a shift in how the internet works and what information it presents.

Web mail services mean that everybody can have an email address; numerous Voice over Internet Protocol (VoIP) and Instant Messaging (IM) services mean that people can communicate live across the globe at no additional cost; the abundance of social networking sites means that anybody can post content to the internet and wireless technology and mobile phones or similar devices can be used to access the internet from any location.

The benefits are numerous. Communication and collaboration between individuals or groups has never been easier: people can share ideas, pictures, music and videos at the click of a button; families can keep in touch across continents; friends can play games in the safety of their own homes. However, this freedom does not come without costs. Decentralisation means that, despite some moderation, there is little control over what is posted to many of the Web 2.0 sites: content is not subject to the scrutiny of webmasters at the time of posting, instead they rely on complaints, often acting only after the damage has been done.

Of increasing concern is the phenomenon of Cyberbullying. According to Wikipedia, Cyberbullying 'is when someone repeatedly makes fun of another person online or repeatedly picks on another person through emails or text messages, or uses online forums and postings online intended to harm, damage, humiliate or isolate another person that they don't like.' [1]

A key difference between bullying and cyberbullying is the technology involved and what that provides the bully. Mobile phones, computers and other devices allow the bully to impersonate a friend of the victim or even remain anonymous. They also enable the bullies to attack their victims in their own home, a place usually considered safe from the more standard playground or office-based bullying. With cyberbullying there is little respite or escape.

The charity website, www.stopcyberbullying.org, argues that cyberbullying affects only children:

“Cyberbullying” is when a child, preteen or teen is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, preteen or teen using the Internet, interactive and digital technologies or mobile phones. It has to have a minor on both sides, or at least have been instigated by a minor against another minor. Once adults become involved, it is plain and simple cyber-harassment or cyberstalking. Adult cyber-harassment or cyberstalking is NEVER called cyberbullying. [2]

Whilst many may disagree with the above differentiation, there is no doubt that cyberbullying, cyber-harassment or cyberstalking are real, rather than virtual problems and are no different in the eyes of the law or society to conventional bullying or harassment.

Cyberbullying and schools:

Everybody can relate to stories about the school bully: from Grange Hill's Gripper Stebson to Tom Brown's arch-enemy, Flashman, bullies have been depicted in school-based fiction for centuries. However, these fictional villains usually get their comeuppance. Real life is often very different, and with cyberbullying the problem is exacerbated. Bullying is no longer restricted to the playground, nor is it restricted to the students or pupils; teachers themselves are increasingly becoming the targets.

Everybody can relate to stories about the school bully: from Grange Hill's Gripper Stebson to Tom Brown's arch-enemy, Flashman, bullies have been depicted in school-based fiction for centuries. However, these fictional villains usually get their comeuppance. Real life is often very different, and with cyberbullying the problem is exacerbated. Bullying is no longer restricted to the playground, nor is it restricted to the students or pupils; teachers themselves are increasingly becoming the targets.

Technology provides the bullies a means by which they can remain undiscovered or anonymous for a long time. Newly-created email addresses or web accounts can be used by the perpetrators to spread their venom or post malicious videos or content to websites such as YouTube, Facebook or RateMyTeacher without fear of detection or reprisal; mobile phones and other internet-enabled devices can be used to show this content on the playground or spread the effect beyond the school gates. As such, bullies believe they can target anybody. One teacher, quoted on www.teachernet.gov.uk, explained how they felt:

"The accusation about me which the students put on their website was horrendous. Within hours it seemed that the whole school had read this message." [3]

A 2008 report by the Association of Teachers and Lecturers (ATL) found that 64% of secondary teachers knew children who had been victims of cyberbullying. It also found that 16% of the teachers themselves had been victims of similar abuse. [4]

For many of the perpetrators and bystanders, cyberbullying is seen as a bit of harmless fun, but the consequences can be extremely damaging and costly, even leading to death – a term increasingly referred to as 'bullycide'. The website www.bullyonline.org publishes a disturbing list of students and teachers who have died or committed suicide as result of bullying. [5]

Cyberbullying in the workplace:

Whilst bullying in the workplace is less common than in schools, it is still a major problem. In March 2008 the BBC reported that bullying as a whole cost the NHS £325 million a year, [6] whilst the Dignity at Work partnership estimates that bullying costs the UK economy as a whole £1.3 billion a year. [7] Their 2007 survey reported that 1 in 10 employees considered themselves to have been victims of cyberbullying, with email and text messages being the principle means of communication and the increased usage of handheld email devices (such as BlackBerrys) being a major contributory factor to the increase in cyberbullying outside of the workplace. [8]

Workplace bullying, cyberstalking or harassment can also be more subtle than a direct attack on a victim. As well as using social networking sites, bullies may choose to use forums, blogs or newsgroups to post upsetting, offensive or simply untrue comments about an individual, especially when they know that the individual and their colleagues use the site as a work resource.

Preventing cyberbullying using technology:

Cyberbullying is simply the appliance of technology to a long-standing social problem. As such, addressing the problem requires a combination of technological and management or social techniques. Below are some recommendations that can help prevent or reduce the impact of cyberbullying at schools and within the workplace from an IT perspective (advice for individuals about bullying and the action they should take as victims, witnesses, parents, teachers, employers or employees is abundant on the internet although some good places to start are: www.digizen.org, www.bullying.co.uk and www.direct.gov.uk).

1. Be responsible: whether a school, a business or a governmental department, it is important for a senior member of the organisation to be ultimately responsible for the establishment and maintenance of an overall acceptable use policy (AUP). Whilst IT departments are generally responsible for implementing and enforcing AUPs, their position is weakened without sponsorship from above.

2. Have an acceptable use policy: an AUP is vital to the success of any IT security strategy. In a corporate or governmental organisation, it may well form the basis of an employee's terms of contract. When monitoring email and internet usage, it is important to let users know that the traffic is being monitored and that they understand what is acceptable and what is not.

3. Enforce the acceptable use policy: any breaches of the AUP should be dealt with equally and appropriately at all levels.

4. Educate users: teaching users about internet and email security is an important part of maintaining an effective AUP. If the users understand why restrictions are in place, then they are more likely to comply willingly. Additionally, the use of well-worded email notifications and web block pages can help users understand why the email they were sent was quarantined or why the website they tried to access was blocked. This can also help reduce the overall impact of IT security on any IT admin staff.

5. Control access to the internet (block anonymous proxies): when users find that their access to the internet is being monitored, some users will try to circumvent any security measures. The most common method is to use an anonymous proxy. Blocking access to these anonymous proxies by identifying their traffic pattern, URL or certificate validity is vital to the effective enforcement of any AUP pertaining to internet access.

6. Control access to websites: restricting access to inappropriate or offensive websites whilst maintaining the use of the internet as an effective resource is the goal of most AUPs. An example is YouTube. Quite often used as a teaching resource in schools, YouTube can also be the vehicle for malice. The ability to block access to the site for one group of individuals (pupils), whilst allowing another (teachers) full access is essential for a balanced policy that allows the Internet to remain a useful tool whilst keeping it safe and secure.

7. Monitor email usage: where possible both internal and internet-originating email should be monitored. Abusive, threatening, offensive or simply hurtful emails can cause a great deal of upset, but are easy to control and monitor. Notifications can be used to inform and educate users about what they have sent and messages can be blocked, preventing the intended recipient from receiving them or preventing inappropriate content being disseminated throughout the school or workplace. Additionally, quarantined messages can be kept to form the basis of any investigation into allegations of bullying or harassment.

8. Block offensive or inappropriate content from being uploaded or downloaded: whether it's in an email, a post on a newsgroup, an entry on a blog or on a website, it's the content that causes the upset or offence. The ability to block emails or access to websites containing this content is paramount to helping prevent cyberbullying. It is also possible to utilise technology to block inappropriate content from being posted or sent in the first place and alert an administrator when any attempt to do so is made.

9. Restrict access to Instant Messaging: instant messaging tools such as MSN Messenger, AIM and GoogleTalk are often seen as a distraction or a waste of time. They can also be used to send or receive files. Blocking these protocols or restricting access to them based on individual users or groups can help enforce an overall approach to reducing cyberbullying.

10. Run regular reports: using reports to understand trends in internet and email use (and abuse) can be very useful in both enforcing and adapting an AUP. 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. Reports on policy breaches or web access can also be used to help back up or repudiate any complaints or allegations of abuse or misbehaviour.

Who is Marshal8e6?

Marshal8e6 is a global provider of Secure Internet Gateway products for organisations of all sizes. The company's complete security portfolio delivers the tools necessary to manage and secure email, Web and the endpoint as well as protect against data leakage. Today, more than 16 million end users in more than 20,000 companies in 96 countries rely on Marshal8e6 solutions to protect their businesses at the email and Web gateway.

Specifically, Marshal8e6 helps educational organisations of any size to:

- Secure networks from misuse and external threats
- Proactively enforce Internet use policies and reduce legal liabilities
- Protect students, staff, inbound and outbound information and the school's reputation
- Comply with legal requirements
- Optimise network bandwidth and improve productivity

Marshal8e6 is the only security company capable of delivering comprehensive content security across multiple delivery platforms, including software, appliances and software-as-a-service (SaaS).

Software Solutions for Education:

MailMarshal Exchange— is one of the few solutions available in the market today to provide email management that filters and manages internal inbox-to-inbox email for educational organisations. It monitors and controls internal office email content that travels within a school, college or university to ensure a safe, productive working environment and **compliance with acceptable use policies**.

WebMarshal— the most complete secure Web gateway solution on the market today. It goes beyond URL filtering to provide comprehensive Web access control and management, complete threat protection (URL, AV and malware filtering) and data leakage prevention in a single, policy-based, easy-to-manage and highly scalable solution.

MailMarshal SMTP— is an email security solution that combines email threat protection, content security, policy enforcement, compliance and data leakage prevention into a highly scalable, flexible, easy-to-manage solution. MailMarshal acts as an email gateway, powered by an unrivalled Defence-in-Depth Anti-Spam Engine, filtering all incoming and outgoing email at the network perimeter.

Marshal EndPoint Security— this is a policy-based enforcement solution that allows only authorised removable media devices to connect to school computers and servers, preventing data leakage and data theft. It enables educational organisations to monitor and control what information goes in and out of the school network via removable media devices such as USB flash drives, iPods, PDAs and CDs.

8e6 Mobile Client—this is a filtering software that works in conjunction with the R3000 mobile solution to filter remote/off-site users such as pupils receiving 1:1 tuition off site. It works with PC and Mac laptops and enables centralised reporting with the 8e6 Enterprise Reporter.

MailMarshal Secure Email Server — is a dedicated policy-based secure email solution that provides encryption, digital signing and deep content inspection of inbound and outbound email messages. It operates with any email gateway that can recognise S/Mime encrypted email, and automatically updates contact details and secure certificate credentials for encryption contact via a centralised server.

MailMarshal Service Provider Edition— a SaaS security solution enabling Managed Service Providers and Internet Service Providers to offer hosted email content security services to any size of school and small office/home office (SOHO) customers. It combines email filtering, anti-spam, anti-virus, anti-pornography, anti-phishing, policy compliance, email archiving and reporting into a centrally managed, highly scalable architecture.

8e6 Professional Edition— a high-performance, scalable appliance-based Internet Security Suite, integrating best-in-class URL filtering, application control, detailed forensic reporting and real-time monitoring and mitigation of Web-based threats. The 8e6 Professional Edition is interoperable and easy to deploy in any network infrastructure—using 8e6's "Pass-by Technology" for zero network impact and fail-safe operation.

8e6 ProxyBlocker— is an appliance specifically designed to work in environments that are not using a Marshal8e6 filtering solution, it detects and blocks Web-based proxies/anonymizers on the fly using "Proxy Pattern Detection" for zero-day protection. This prevents students from using proxy sites to bypass school Web filters that are designed to prevent them for accessing unsuitable websites from the school network.

MailMarshal e10000— is an award-winning security appliance built upon the same platform and policy engine as MailMarshal SMTP software that combines the ease of installation and low administration overhead of a hardware appliance with the flexibility, scalability and depth of functionality of a software solution.

For more information, visit www.marshal8e6.com

References:

- [1] <http://en.wikipedia.org/wiki/Cyberbullying>
- [2] http://www.stopcyberbullying.org/what_is_cyberbullying_exactly.html
- [3] <http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/>
- [4] <http://www.atl.org.uk/Images/17%20March%202008%20-%20Annual%20conf%20-%20Cyberbullying%20March%202008%20FINAL.pdf>
- [5] <http://www.bullyonline.org/schoolbully/cases.htm>
- [6] <http://news.bbc.co.uk/1/hi/programmes/breakfast/7302767.stm>
- [7] <http://www.dignityatwork.org/uploads/files/the-business-case.pdf>
- [8] <http://www.personneltoday.com/articles/2007/07/26/41707/one+in+10+workers+experiences+cyberbullying+in+the+workplace.html>



Corporate Headquarters

Marshal8e6

828 West Taft Avenue
Orange, CA 92865
United States

Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters

Marshal8e6

Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848 080
Fax: +44 (0) 1256 848 060

Asia-Pacific

Marshal8e6

Suite 1, Level 1, Building C
Millennium Center
600 Great South Road
Auckland, New Zealand

Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720