Chapter 6
Cyberbullying:
Keeping Our Children Safe in the 21st Century

Iris Reychav
Ariel University, Israel

Shraga Sukenik
Ariel University, Israel

ABSTRACT

In the 21st century, thus far, we have seen a growing dependence on and usage of the Internet and communications technology. This has been especially true for youth who spend much of their time communicating in cyber space. This allows for developing and maintaining relationships. At the same time, an ugly and dangerous phenomenon called cyber bullying has reared its head. In this chapter, the authors discuss various aspects of this phenomenon, including, but not limited to, incidence rates, comparison to traditional bullying, risk factors for being involved either as a bully or a victim, how it affects its victims, relevant legal aspects, and most importantly, how to defend against it. The discussion of coping strategies is especially detailed and provide suggestions for schools, parents, bystanders, victims, and broader society.

INTRODUCTION

In recent years we have seen many wonders that can be accomplished through information and communications technology. Young people have especially benefited from these advances, accruing many advantages from the Internet and mobile phones such as access to educational information, resources and collaborative learning networks, the development and maintenance of relationships and friendships with their peers, and an outlet for creativity, to name a few (Kowalski, Limber, & Agatston, 2012). However, there have also been risks and dangers that have accompanied the expansion of the 'virtual' world. Cyberbullying is one of the online risks youth face, and the one they are most likely to encounter (Livingstone, Haddon, Gorzig, & Olafsson, 2011).

Cyberbullying is defined as actions that use information and communication technologies to

support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm another or others (Dilmac, 2009). These crimes have been shown to have serious consequences for their victims. For example, victims will isolate themselves socially, display more anger and depression, and in some cases will be driven to suicide, as was the case with Phoebe Prince (ABC News, 2010), Megan Meier (New York Times, 2007), and several others. Cyberbullying has become a major concern to modern society (Martin & Rice, 2011). One way this is reflected is that the general awareness and media attention have grown in the last decade (Dooley, Pyżalski, & Cross, 2009; Patchin & Hinduja, 2011). One needs to address the problem of cyber bullying broadly and systematically, involving peers, teachers, school administrators, mental health professionals, law enforcement, parents, and of course the victim (Mishna et al, 2010). We will address each of these parties and their respective roles in cyber bullying prevention (see Figure 1).

We will present a "multi-pronged defense" in which all members and groups in society can play a part in preventing cyber bullying (e.g. schools, law enforcement agencies, bystanders).

Before one can discuss ways of preventing cyber bullying we first have to understand the phenomenon better. This includes defining the relevant terms and how it differs from traditional bullying, its prevalence, risk factors for being a bully or victim, the negative effects on the cyber victim, and the like. To this end, this chapter will include definitions and typology of cyber bullying, rate of incidence, possible motives for the perpetrators, risk factors for both bully and victim, negative effects on cyber victims, the similarities and differences to traditional bullying, the legal aspects involved in combating and prosecuting cyber bullying, and most importantly, strategies for preventing and coping with cyber bullying.

BACKGROUND

Many definitions of cyber bullying have been used, which is problematic in terms of conceptualization and challenges our ability to compare studies in this field. The definition which appears to have a great degree of adherence, and will be adopted in this chapter as well, is that of Dilmac (2009) *"an individual or a group willfully using information and communication involving electronic technologies to facilitate deliberate and repeated harassment or threat to another individual or group by sending or posting cruel text and/or graphics using technological means".* Cassidy, Faucher, & Jackson's (2013) quote a popular definition (Smith, Mahdavi, Carvalho, Fisher, Russell, & Tippett, 2008) that adds the element of a victim who cannot easily defend him or herself.

A cyber bully can either act alone or get others to assist. Assisting a cyber bully is an act called "cyber bullying by proxy". According to Anderson (2010) cyber bullying refers specifically to situations in which both parties are children. Once an adult becomes involved, it is known as cyber harassment or cyber stalking. Cyberbullying by proxy may involve adults and that makes it all the more dangerous.

Someone can engage in direct or indirect cyber bullying. Direct cyber bullying occurs where the cyber bully directs the electronic communications directly at the victim while direct cyber bullying occurs privately between the bully and the victim. Indirect cyber bullying occurs when the bully posts the bullying message, video, etc. on a public platform in cyber space (e.g. Facebook, a blog, MySpace, etc.) (Brenner & Rehberg, 2009).

Cyber bullies will use methods such as cyber stalking, and cyber harassment to achieve their aims.

Cyberstalking uses the Internet, email or other electronic communications to stalk, generally referring to a pattern of threatening or malicious

Related Content

An Adaptive JPEG Steganographic Scheme Based on the Block Entropy of DCT Coefficients
Chang Wang, Jiangqun Ni, Chuntao Wangand Ruiyu Zhang (2012). *International Journal of Digital Crime and Forensics (pp. 13-27).*
www.irma-international.org/article/adaptive-jpeg-steganographic-scheme-based/68407

Unexpected Artifacts in a Digital Photograph
Matthew J. Sorell (2011). *New Technologies for Digital Crime and Forensics: Devices, Applications, and Software (pp. 211-223).*
www.irma-international.org/chapter/unexpected-artifacts-digital-photograph/52855

Security Architecture and Forensic Awareness in Virtualized Environments
Diane Barrett (2013). *Cybercrime and Cloud Forensics: Applications for Investigation Processes (pp. 129-155).*
www.irma-international.org/chapter/security-architecture-forensic-awareness-virtualized/73961

Le Grand Saint-Antoine's Cargo: A Worst Alleged Case of Corruption in Human History
Jean Michel Rocchiand Ivan Topalovic (2023). *Theory and Practice of Illegitimate Finance (pp. 106-128).*
www.irma-international.org/chapter/le-grand-saint-antoines-cargo/330627

Core Models for State-of-the-Art Microscopic Traffic Simulation and Kay Elements for Applications
Heng Wei (2008). *Artificial Crime Analysis Systems: Using Computer Simulations and Geographic Information Systems (pp. 92-124).*
www.irma-international.org/chapter/core-models-state-art-microscopic/5260