ROMAN CATHOLIC
ARCHDIOCESE of DUBUQUE
Share Jesus Love

Office of Protection of Children

P.O. Box 479 • Dubuque, Iowa 52004-0479
Phone (563) 556-2580 FAX (563) 556-5464
www.dbqarch.org

Preventing Cyberbullying in Online Gaming, Part 2

By Sameer Hinduja, Ph.D.

In Part 1 of this article, we shined a spotlight on the ubiquitous participation in online gaming in the lives of the youth we care for and seek to protect. The pace of online gaming is only growing, and it provides benefits many adults often overlook. That said, there is a small but real chance of victimization that can befall kids when they play and interact with others via their phones, tablets, laptops, desktops and gaming consoles.

In order to equip you to best educate and help protect young people from personal vulnerabilities while playing, we are sharing a number of best practices you can immediately adopt and convey to the youth you supervise. Previously, we encouraged you to pursue familiarity with the games youth play, highlight and guard against online provocation by "trolls" and set specific limits to promote discipline and balance. Below, we share seven additional safety tips that should round out your ability to be involved, respond to incidents and eventually prevent most of them from occurring.

Familiarize yourself with rating systems

The gaming industry is somewhat regulated by a number of third party rating systems that assess and represent the games created and released for the masses. These rating systems contain information such as categories, content and details on possible interaction with other gamers. The most respected ratings from the Entertainment Software Rating Board (ESRB) have three components:

Categories indicate the level of maturity needed to play the game in question (i.e., to help you determine whether the game is age-appropriate).

Content means whether the game contains profanity, nudity, etc.

Interaction means whether the game allows for contact from another gamer, provides the ability to share personal information or to pinpoint one's location.

We recommend you clearly understand the ratings for every game the children in your life plays, and make usage decisions accordingly. Please refer toCommonSenseMedia.org to help fill in any knowledge gaps as it relates to game ratings.

Report It

A helpful way to teach children about handling problems is to encourage them to report issues when they arise. Internet service providers and gaming networks have systems set up to field complaints of abuse

and then investigate them (in conjunction with law enforcement, when necessary). Caring adults should encourage kids to always take a few seconds to report other players within the game itself if they are being abusive or legitimately problematic. You can also work more specifically and individually with these companies, depending on the severity of harassment experienced. As per the ESRB, those who encounter unscrupulous gamers online should include as much information (nicknames, detailed patterns of behavior, online locations) and digital evidence as possible (screenshots, logs) to help the organizations investigate these matters.

> *I was on Clash of Clans, it's an app that I had on my phone. I was leaving my brother's clan because they were picking on me and finally I got kicked out. I asked if I could join a clan on global chat. I got lots of comments like 'Wow, you suck' and I got a lot worse comments that which [sic] I would not like to share.*

Practice safe password practices

As we've seen in numerous instances over recent months (e.g., the Ashley Madison situation[1]), hackers have become more and more prevalent in today's society. One way to protect a young person's account is to teach them to maintain strong passwords. Specifically, passwords should minimally have at least eight characters containing upper and lower case letters, unsequenced numbers, and symbols (e.g., $, %, &, #). This is a simple but effective way to ensure passwords are stronger. They should never be a nickname, birthdate, or something else that a person close to you might know or be able to find out. Many youth share passwords for purposes of convenience or bonding with one another, but that simply should not happen. Kids should not trust anyone with their passwords or personal information. Finally, parents should encourage kids not to use the same passwords across multiple gaming accounts. This is because if one account is compromised, others quickly may follow.

> *Last night on Twitch TV, my 13 yr. old son and his brother were approached by a group saying audio [was] not working. They claimed to be twitch tech support. They said download X, give me your stream key, and friend me on skype. The download crashed my 11 year old's computer. My 13 yr. old skype called Jordan.Daniely or Jordan at Twitch. When told the problem the group laughed and offered more fixes and threats. They were on the Skype call for over an hour. They wanted photos and recorded the boy's reaction to the crash. They attached pornography to the boy's twitch stream. They kept skype calling over 100 times again in the morning.*

Control your online gaming experience

There are a number of customizable features available within each gaming environment. For example, Internet access can be completely disabled to prevent any online connectivity. If that is considered to be too extreme, we encourage families to allow participation on the online gaming network but with voice chat and text chat switched off. This basically means that the youth can play with/against other gamers, but not talk with them. If you want to allow some interactivity, however, all game consoles allow you to choose and/or restrict those who can contact you through their equivalent of a "buddy list." Additionally, users can always "mute" specific people during a game. Please visit A Guide to Setting Up Parental Controls for Video Games (from the PTA and the ESRB), or Parental Controls on Xbox360™, Nintendo® Wii™ and PlayStation® 3 (from British Telecom) for specific instructions for each console.

Refrain from divulging personal information

Kids who interact with others online should never give out their personal information to strangers or even friends. Protecting personal information on the Internet is of paramount importance, and should never be disclosed. Information such as a person's full name, physical address, phone, student ID and social security numbers should (obviously) never be shared in gaming environments. Furthermore, screennames should be used to provide a level of pseudonymity and youth should upload an avatar image into their profile for privacy reasons, instead of using their actual photo.

As an example of why kids should not trust others online, Henry, who is an 11-year-old player of the game Destiny, allowed a stranger to use his account via a feature on PS4's Share Play his gaming console feature. The man was supposed to help Henry, but instead, the stranger not only deleted two of Henry's three high-level characters (that he had spent months developing, training, and growing), but also began deleting his special weapons as well (which he had spent his hard-earned virtual money on). This was all caught on video. Once Henry realized what was happening, he switched off his PS4 console, but he was too late. At the end of the video, you can hear Henry sobbing and clearly devastated. Henry's parents had the following response:

> *As Henry's parents, we are constantly reminding him to be careful, to never share your personal information, to always be on the lookout. But the truth is, no matter how many times a parent says this to a kid, when you're in the actual situation, it's easier to trust people you think are your friends because someone you actually know in real life vouches for them.*[2]

Avoid Mods

In the gaming world, *mod* is short for *modification*. Some online gamers offer mods to others, which allows a user to modify the content of a game and release certain (often adult-oriented) features or functionality, or otherwise provide a cheat, shortcut or other unethical benefit. These are available for many games. Kids should be wary of these game-related downloads from third parties. While it is tempting to play around with such modifications to see what they can do, they can introduce malicious code into the game, console, or portable device (making it unstable or even unusable).

Keep your consoles updated, clean and protected.

A final suggestion to promote safe gaming: ensure the latest firmware is updated in your console and device manufacturers to patch and secure any vulnerabilities in the operating system. Also, make sure the home network is behind a firewall to avoid viruses or worms from being introduced into the systems via the Internet connection. Lastly, use a strong password to protect the wireless Internet connection to prevent strangers from accessing the network and devices.

The gaming industry is growing at an incredible pace, and the technology involved is getting better with every passing year. Indeed, the environments in which individuals play together online will probably become more realistic, and the ways in which interaction via their devices can occur in the future are perhaps beyond our current imagination. Regardless of the changes that lay ahead, the aforementioned tips can help safeguard children's' participation. Encourage healthy usage, and then periodically check to make sure the strategies are effective and being followed. Hopefully in time, these safety measures will become standard practice to help youth stay protected against preventable online victimization while fostering a gratifying experience for all involved.

A helpful resource may be the Cyberbullying Research Center (cyberbullying.org) that has numerous free resources available.

References:

1. http://fortune.com/2015/08/26/ashley-madison-hack/

2. http://www.polygon.com/2015/2/23/8090061/destiny-characters-deleted-ps4-share-play