# **Online Gaming Risks and Kids: What to Know and How to Protect Them**

**Source**: [www.webroot.com](http://www.webroot.com)

**By**: Levar Battle

Online games aren’t new. Consumers have been playing them since as [early as 1960](https://thriveglobal.com/stories/the-history-of-online-gaming-and-its-advancement-today/). However, the market is evolving—games that used to require the computing power of dedicated desktops can now be powered by smartphones, and online gaming participation has skyrocketed. This unfortunately means that the dangers of online gaming have evolved as well. We’ve examined the top threats that parents need to know about to keep their kids safe while gaming online.

## **Online Bullying and Harassment**

A recent study shows that [65% of players](https://www.adl.org/news/press-releases/two-thirds-of-us-online-gamers-have-experienced-severe-harassment-new-adl-study) who participate in online gaming have been harassed; a statistic that does not bode well for underage gamers. Your first instinct may be to try to prevent your child from participating in online gaming altogether, but this may cause them to sneak playing time without your knowledge. A stronger choice would be to talk with your kids and prepare them for the types of negative behavior they may experience online, and to make sure they know they can come to you if they are being harassed. It’s also important to explain the impact that online bullying can have on others, and to set firm consequences if you catch your child participating in harassment or abusive language. Regulating the use of headsets can help prevent both your child’s exposure to and participation in online harassment.

Two types of harassment specific to online experiences go a step beyond what you would expect from online bullying: doxxing and swatting. Doxxing is when one or more online participants seek personal, identifying information on a particular user for blackmail or intimidation purposes. Doxxing can often lead to the release of real names, phone numbers, home addresses, employer information, and more. Swatting is a form of harassment that uses doxxing techniques to create an actual, tangible threat. A harasser will call in a threat to a doxxed user’s local law enforcement, often claiming there is a kidnapping or hostage situation at the victim’s address. This may bring a large SWAT response unit to descend upon the address.

Keeping an open line of communication about your kid’s gaming experiences is critical. Swatting can happen over seemingly innocuous events. One of the most notorious examples followed a dispute [over a $1.50 bet](https://www.latimes.com/nation/la-na-tyler-barriss-swatting-sentencing-20190329-story.html) in “Call of Duty: WWII.”  
  
Pro tip: one is only vulnerable to doxxing and swatting if a harasser can link identifying information back to the targeted gamer. Educating your kids on digital privacy best practices is one of the strongest security measures you can take against these forms of online harassment.

## **Viruses and Malware**

As with almost every digital experience, you’ll find specific cybersecurity threats associated with the online gaming landscape. We asked Tyler Moffitt, Webroot security analyst, for his thoughts on the malware threats associated with online gaming.

“The thing kids should really watch out for with games is the temptation to cheat,” explains Moffit. “In popular games like Fortnite and PUBG, ‘aimbots’ are very common, as they allow the player to get headshots they normally wouldn’t be able to make. However, many of the aimbots that kids download from forums are packed with malware—usually  ransomware or info-stealing Trojans. What’s worse: a lot of young gamers also don’t run antivirus because they think it will make the game slower.”

The bottom line: cheating at online games isn’t just ethically icky, it makes you a [proven target for hackers](https://www.fastcompany.com/90246549/fortnite-cheaters-are-being-targeted-with-malware). Make sure your kids know the real cost of “free” cheats.

## **Phishing Scams and Account Takeovers**

Where there’s money, there are scammers. With more than [1 billion gamers](https://venturebeat.com/2018/06/07/fraud-is-taking-the-fun-out-of-video-games-scams-spam-account-takeovers/) actively spending money not just on games, but in games, it’s no surprise that phishing scams have become commonplace in gaming communities. One of the most prevalent phishing tactics in gaming: account takeovers are often prompted by a risky link click on a gaming forum, or a compromised account sending out phishing links to other users. Once the hacker has control of the account, they can run up fraudulent charges to any attached credit cards or, in some cases, sell the compromised account (particularly if it contains valuable items or character skins). Young gamers are especially at risk for these hacks. In these cases, chances are that any credit cards attached to gaming accounts belong to you, not your kids, so young gamers aren’t going to notice who’s spending your hard-earned funds.

## **Keeping Your Kids Safe**

You’ll find plenty of tools to help your kids stay secure while gaming. Reliable [antivirus software](https://www.fastcompany.com/90246549/fortnite-cheaters-are-being-targeted-with-malware) installed and up-to-date on all of your household smart devices can protect your family from malicious software. Additionally, wrapping your household web traffic in the secure encryption of a [trusted VPN](https://www.webroot.com/us/en/home/products/vpn-wifi-security) could reduce doxxing potential. But your kids will only find true security through digital literacy. Start conversations with them not just about online bullying, but about recognizing cybersecurity threats and phishing scams. If you’re having a hard time connecting with them over the threat, remind them that it’s not just your wallet on the line. Account takeovers are now all too common, and no kid wants to see their Fortnite skins sold for a stranger’s profit. Also, always be sure to exercise caution in giving out information on the internet. Even small, seemingly irrelevant pieces of information could be used to pull up Facebook or other user account pages to grab even more personal data.

To keep your kids educated about online gaming risks, it’s important to educate yourself as well.