Internet Safety for Kids: Top 7 Online Gaming Dangers

According to research from the Entertainment Software Association, 70% of families have at least one child who plays video games. Mobile is becoming a critical segment of the game industry. NPD Group reports that 59% of U.S. gamers age 2+ play across devices, on dedicated gaming consoles, desktops, laptops or mobile devices. And 34% of gamers who play exclusively one system do so on a mobile device.

While online gaming can provide quality social interaction, there's also a darker side. From cyber bullying to online predators to hidden costs, there are many concerns when it comes to playing video games online, especially for children. The most important thing a parent can do is to establish a dialogue about safe online usage at a young age and build upon that as your children get older. When they understand the risks and the importance of security, children are more likely to come to you with red flags, alarms or smaller things that worry them.

Here's a list of the top seven dangers and simple tips to keep your kids safe online.

1. **Cyber bullying**

   For many kids, the ability to escape into an online world offers relief from real life—no one knows who they are, what school they attend or what they look like. This anonymity cuts both ways, however. This may start out as the gamer version of poor sportsmanship. As noted by [Get Safe Online](), some players take advantage of their anonymity to "grief" other players by deliberately making the game less enjoyable. This could include "kill stealing," which is when griefers conquer or capture needed quest targets before other players can get to them; or "chaining" groups of high-level challenges to block the progress of low-level players, causing them to die.

In some cases, griefing escalates to cyber bullying. Although cyber bullying sadly has countless forms, some forms are particular to gaming platforms. In "whispering" cyber bullies target players directly with hurtful and harmful messages, or by spamming global chat channels with derogatory comments about their victims. According to Stay Safe Online, it's critical for kids and parents to understand their options. Most games allow players to "block" chat and messages from other users, and in some cases, the bully's words or actions may be a violation of the game's terms of service. It's always a good idea to write down or take a screenshot of any offensive conversation and report it to game administrators.

2. **Privacy Problems**

   Stay Safe Online also recommends that kids never create usernames that are derivatives of their real names, or that might reveal any other personally identifiable information (PII), such as their location or age. According to US-CERT, the social nature of online gaming allows cyber criminals to manipulate conversations. They may single out your child in a general chat channel and then start sending personal messages that ask for detailed personal information. By piecing together data from games and other sources, hackers may be able to access other existing accounts such as social media or establish new accounts—even entire digital identities—in your child's name. As in any online forum, never give away any personal information and be sure to vary usernames and passwords are across different games, platforms and accounts.

3. **Personal Information on Consoles, Computers and Devices**

   Another online gaming danger comes from consoles or PCs themselves. When they've outlived their usefulness, many families take these devices to the local electronics recycling center or sell them on swap sites. Users often forget how much personal information is in the files saved to these devices and fail to delete their profiles and information, putting their financial and private data at risk. Before getting rid of any computer, game console, tablet or smartphone, you should wipe all personal data from and then perform a factory reset.

   The specific tools or procedures needed might vary depending on the type of device, so it's important to research this for each device. Also, remember that some devices might include storage areas that aren't affected by the device's erase functions. If a device uses computer-compatible storage drives, like SD cards, connect them to your computer and securely erase the data. For computers, don't rely on the "Delete" function or even reformatting. These features are designed to permanently erase all user data from disk drives. Instead, you should use a program that completely removes data by overwriting the data multiple times.

4. **Webcam Worries**

Webcams have been hacking targets since they entered the scene. At first webcams were physically separate peripherals, manually added by end users and often left unprotected and with their default factory settings. The exploits were many and easy. Today, with many devices, from laptops to tablets to smartphones featuring built-in webcams, reports of webcam hacks continue to be regularevents. Whether internal or external, any connected recording device—such as a webcam or microphone—can be controlled remotely by attackers and used to exploit your children. To help mitigate this risk, use cyber security software that provides real-time and scheduled system scans for malware. Ensure that all webcams use "off" as their default setting and make use of physical shields, be they built-in camera covers or even a piece of opaque tape.

5. **Online Predators**

Online predators are typically older gamers who use video games to lure and groom younger victims. This can culminate in inappropriate messages, webcam chats or even face-to-face meetings that could lead to sexual exploitation. According to Internet Safety 101, online gaming gives predators the chance to build a kind of shared online experience, in effect becoming the child's defender, teammate and ally. After defeating a tough opponent or exploring a new level of a game, predators form a bond with younger gamers based on these common experiences and leverage them to venture into more personal territory. In many cases, predators seek to isolate children by splitting them from them parents and real-life friends by taking up the mantle of the "only person who really understands them." Combating this problem means talking to your children about online risks and monitoring their gameplay closely.

6. **Hidden Fees**

   Dangerous online games have many forms and tricks. Some online games use the "freemium" model, which means they give you some content for free, however, for full game features, functions and access payment is required. So-called free mobile games are big business, generating over $61 billion in 2018 alone. A few years ago, the freemium business model offered to remove in-app ads for a modest one-time fee. Since then, the freemium model has rapidly evolved to offer subscriptions, expanded functionality, virtual currencies, weaponry, special abilities or other accessories in exchange for credit payments. In most cases, these games require users to attach a credit card to their gaming profile. Their card is automatically charged whenever users purchase new items or services.

   The solution is simple. Never give out your card number for any freemium games. If your child is playing more traditional subscription-based games, or games that run through services like Apple or Google Play, activate the purchase password feature these providers offer in their account settings menu. It's a good idea to regularly check your credit card bills to make sure you're not being charged for purchases you didn't approve. If you allow your children to use your smartphone or tablet, you should consider switching off "in-app updates," to prevent your children from racking up huge bills for in-app purchases without even realizing it.

7. **Malware**

Trojans may modify a legitimate app and upload the malicious version to Google Play or another legitimate marketplace. Malware such as adware and Trojans that convert infected machines into zombies in larger botnets continue to plague even the most reputable app marketplaces. Often malware operates on a delay timer, so victims don't connect their online gaming to the attack. The lesson here is to mindful of which apps you download. Malware can be hosted by or simply masquerade as a legitimate app. Three basic steps to minimizing malware risks are as follows:

1–Pay attention to recent reviews and news stories

2–Research the game developers as well as the vendor or marketplace

3–Use your cyber security software to scan the files when you download them to your computer or mobile device

Make sure you discuss and approve all your children's gaming and downloads. The importance of reputable cross-device cyber security software cannot be overstated. Playing online isn't all fun and games—children are at risk from bullying, identity theft, credit card fraud and even sexual exploitation. Make sure to talk to your children about these risks.

Only by establishing a dialogue at an early age, will they be prepared to avoid these threats. Don't lose out—look for warning signs, understand the risks and take an active interest in your kids' online gaming habits.

What’s the best way to ensure your children’s safety from online gaming dangers?

Go beyond monitoring and discussions—**regularly play video games with your children**. Not a gamer? Let your child be your teacher. Gaming with your children not only ensures an accurate understanding and truly open communication, it strengthens your bond by through shared experiences and the tacit validation of engaging with your children in their forums and activities of their choice.

Related articles and resources:

- What is cyber security?
- Internet Safety for Kids: Top 7 Internet Threats
- Internet Safety for Kids: Tips for Parents of Twitter Teens
- Internet Safety for Kids: 5 Quick Tips for Snapchat Security
- Internet Safety for Kids: Terrifying Stats & 10 Ways to Stop Cyber bullying Now
- What is social engineering?