ONLINE GAMING

IN-GAME CURRENCY

Understand the mechanism of the points and bonuses system. Some games require players to play the game every day to claim the rewards. This create pressures to continue playing beyond the intended time.

Games where players can purchase currency or credits using real money may offer high incentive to players for doing so. Players can advance quicker or buy the tools that would give them the advantage over other players. The incentives offerings mean players can easily overspend and be encouraged to make repeat purchases.

Watch out for “fermium” model where gamers may get some content for free but are required to pay to access other portions of the game. Also, be aware that games today are subjected to a range of targeted advertising campaigns.

Remember to look out for secured payment methods including secure websites with https:// and padlock symbol in the URL bar of the browser.

Tips for parents

1. Have a dialogue with your child on sensible spending for the games they are into and about the value of money. If your child is determined to spend money in the game and you agree to it, you may want to guide them through the purchase.
2. If your children use your smartphone to play games on it be sure to turn off “in-app updates” to prevent you or your children from racking up huge bills for in-app purchases without even realizing it.

MALWARE AND FAKE APPS

Just like any Internet users, online gaming players are exposed to threats by cybercriminals in manipulating them into clicking unknown links that lead to malicious software or downloading and installing them.

Malware may modify legitimate apps and upload the malicious version to Google Play or another legitimate marketplace. Once downloaded and activated, hackers will be able to spy on you; steal your sensitive data (including your game passwords!); hold access to your data at ransom; and control your device and make it a part of a larger “botnet”.

Also, avoid installing a crack to bypass legal permission to play the game. Hackers usually embed malware in the software.

Therefore, it is important to download only from reputable sources, read reviews, and research the developers before downloading any apps.

<u>Tips for parents</u>

Make sure you are the only one approving all mobile downloads and take the time to install a reputable mobile anti-malware scanner so you can r regularly check all devises in your home.

MANAGING YOUR TIME

It is important to understand that unless you are playing in the e-games or produce gaming videos fulltime on YouTube, the purpose of playing the online games is to relax and be entertained. Most players see gaming as an escape from the real world, such as the stress at workplace or studying. It is like having a cheat day in your diet regime, or the unjustified shopping, or watching dramas or sports channels.

Just like any entertainment activities, gaming needs to be minimized and kept under control so that it would not interfere with real life productivity.

Gaming should serve as a reward; eliminating it creates a vacuum that could implode in the form of excessive gaming. The balancing act is delicate and here are some ways you can do it:

> Define what is important in your life? Your job/study or gaming?
>
> Set the time, either hourly or match based
>
> Turn gaming into an event.
>
> The short and controlled bursts of gaming will satisfy your need for relaxation without letting you fall into a downward spiral of unproductiveness. Also, having limited time would make you want to make sure every minute counts.
>
> Set a timer and put it away from your gaming area. When it rings, you will need to get up to turn it off.
>
> Get someone to hold you accountable. If you live with someone (not a gamer), explain them your plan and ask them to make you stop playing.

<u>Tips for parents</u>

Agreeing on the time your children can spend gaming might be ideal, but parents need to understand the nature of the game for the measure to be effective. Talk to you children to get a better idea on how you can manage their time in that specific game. The stop time can perhaps be the number of quests completed or number of team matches played. Coming to terms together is better than setting a strict rule and demanding them to adhere to it.

BULLYING

With the ability to hide real life identity and be anonymous, some gamers took advantage of this feature to make gaming an unpleasant experience to other gamers. These bullies are called “griefers”. While they engage in normal competitive gaming moves, this can also escalate to bullying acts such as “whispering” players directly with hurtful and harmful messages, or spamming global chats channels with derogatory comments about their victims.

Most games allow players to “block” chat and messages from other users and in some cases, the bully’s actions may be in violation of the games terms and conditions. Take a screenshot of any offensive conversation and report it to the game admin.

Tips for parents

It is important for the young gamers and parents to know what can be done to overcome the situation. Study the safety features in the game with your child and let them know that they have the right to a pleasant and enjoyable experience in the game.

PRIVACY PROBLEMS

As a gaming rule of thumb, never create user names that are derivatives of their real names, or that might give away their location or age. As the social nature of online gaming makes it easy for cybercriminal to manipulate conversations, players might be singled out to receive personal message from the criminals asking for personal information. The goal here is to get as much information as possible so that they can open accounts with your details or gain access to your child’s existing account. To prevent this, never give away personal information and make sure that login details are different across different games and gaming sites.

Tips for parents

It might be difficult for your young gamer to come up with login details for across different games and gaming sites. Help them out by creating passwords that are strong yet easy to remember i.e. they can represent things or experiences that only they and you know of. It might be difficult to remember several login details (in addition to yours!), so if you must write them down, make sure you keep them in a secured and safe place.

PERSONAL INFORMATION LEFT ON CONSOLES AND PCS

Once the game consoles or PCs have outlived their usefulness, they are usually discarded without any safety precaution. Users often forget to delete their files and personal information, in turn putting their financial and private lives at risk. You should wipe all personal data from games consoles, tablets and smartphones and then perform a factory reset. The specific tools or procedures needed might vary depending on the type of device, so it is 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 the device includes PC-compatible storage drives (e.g., SD cards), connect them to your PC and securely erase the data. For PCs, don't just rely on the "Delete" function or even formatting, since these will not actually remove data from the drive. Instead, you should use a program that removes data by overwriting the data multiple times.

Tips for parents

Help your child to erase or reformat their game consoles or devices.

Refer to the steps above on how to do it.

SMILE, YOU’RE ON CANDID CAMERA!

It is easy for anyone to search online on how to hack into your webcam and control it. Once the Remote Access Trojan or RAT spyware is installed in your PC, the cyber criminals can see anything you do online, read your messages or emails, that social media postings, and capture your screen and keystrokes. Basically, they have full control of what they want to see through your webcam without you even knowing about it and even your screen is turned off.

So here’s how you can prevent webcam hacking:

Cover your webcam with paper or tape, or disable it if you don’t use it.

- For Android phones: Go to “Settings” > “Apps” > “Camera” > “Disable” option
- For iPhone: Go to “Settings” > “General” > “Restrictions” > flip Camera to OFF– Note: this will automatically disable FaceTime as well.

Always use an up-to-date antivirus, and make sure your firewall is enabled

Only use your cameras over a secure internet connection

Keep your operating system, browser, and software up to date

Don’t click on suspicious links and don’t chat with strangers online

Be wary of fake emails which appear to be sent from trusted sources and ask you to download attachments, click on a link, or disclose any personal details

Your smartphone needs protection too, so set up a strong passcode, use an antivirus, and keep your software up to date

Tips for parents

Any connected device—such as a webcam or audio device—could be controlled by attackers and used to exploit your children. To help mitigate this risk, make sure to scan your system for malware regularly, and ensure that your webcam's default setting is "off". Other than that, please refer to the tips above.

SEXUAL HARASSMENTS

As a type of bullying behaviours, sexual harassments are quite rampant in the online gaming world. In a study titled “Sexism in Video Games” by Emily Matthew, 80% of 874 respondents polled believe sexism is rampant in the gaming community, and 35% have been on the receiving end of sexual harassment while playing online. Women reported to be harassed four times more than men were, and were much more likely to quite a game temporarily or even permanently because of harassments. As a result, 68% of women reportedly have kept their sexual identity secret on occasion in order to avoid sexual harassment.

The harassments and constant sexual overtures can negatively affect a player, making what supposed to be an entertaining activity into a nightmare. What players can do to help themselves out of the situation is to temporarily close the account and change their gaming identity, or contact the admin and report the bully.

For other players, try to stop the harassments and report them to the admin. Be an upstander, not a bystander.

Tips for parents

Online Predators

The predators are typically older gamers who use online gaming to lure and groom younger victims. The end result may be inappropriate messages, webcam chats, sexual exploitation or even recruitment to terrorist groups or organized crimes. According to Internet Safety 101, online gaming provides a chance for predators to form bonding with their victims through shared online experience. In many cases, predators seek to turn the victims against their parents by instilling in them that “only they (the predator) understand them”.

Parents can build their children’s resilience against online grooming by talking to them about online risks and monitoring the game play closely. Most importantly, parents should understand that an open communication channel between them and their children, and the confidence their children have on that trust are the best protection they can afford their children.