How Big Of An Issue Is Game Cyber Security?

"Finish him!.," " Boomshakalaka!". "I need a weapon!". These expressions and more aren't new to you if you are familiar with the game world.

A fantastic thing about games is that it's versatile; there is always a game suited for everyone. Unfortunately, for gamers, there is always a threat to their security.

Is this noteworthy? What threatens game cybersecurity? How can gamers safeguard themselves? This article will discuss this and more.

Cyber attacks are prevalent in the game industry. Studies show that every 39 seconds, a cyberattack occurs. Over 6.3 billion attacks happen globally.

Threats like phishing, cyberbullying, fraud, and identity theft are rampant in the gaming space.

You can shield yourself from these threats by using strong passwords, reporting bullying, and using multiple-factor authentications to secure your information.

Why Is Gaming Cyber Security threatened?

There is a constant threat to cybersecurity like every space. It's worse for the gaming industry because it is one of the largest entertainment platforms.

With the onset of the pandemic, game platforms became a source of consolation. For some people, game platforms are a source of income.

Two main reasons why it's threatened are:

- Digital Value

Gamers who have established accounts with significant in-game currencies or access to unique and rare game assets are valuable.

Rare assets are a commodity that can fetch good money in the real world. The game currency is valuable both on the gaming sites and outside it.
Game creators invest a lot of time and resources into creating games, making the gaming industry a vast fortune.

- Data

When gamers sign into a gaming platform, either through their computer or a mobile device, they provide user details.
User information provided is valuable to both the platform owners and potential hackers. The more data provided, the more valuable the individual is.

Now that we have seen two important reasons why gaming cybersecurity is under attack, what threats are you likely to face?

What Are The Threats To Gaming Cybersecurity?

There are a lot of threats gamers face; let's talk about a few of them:

- Phishing

Phishing refers to a type of social engineering where attackers assume the identity of trusted entities or organizations. They send emails or messages requiring them to reveal sensitive information.

Phishing could be in the form of ransomware or links to malicious sites. They might replicate a popular game site or platform. Then request users to change their passwords or other login details on the new site threatening users with the loss of their accounts or game levels.

- Identity Theft

Identity theft is widespread in the gaming world. Most gamers are minors, teenagers, or young adults. These may be partially or wholly unaware of the dangers of revealing their identity to strangers.

Take the example of Lisa Lockwood, whose son's identity was stolen from an online game site and used to apply for about seven different loans.

Usually, attackers target "game lords," that is, individuals who are doing very well in the game. They have high scores, and they have rare assets the game gives.
Hackers may befriend these young ones and build a relationship with them. Gradually they build trust and lure them into revealing personal information.

- Loss of Level Progress In The Game

A glitch in a game system can significantly benefit a hacker. Hackers can easily use software to make mathematically impossible scores for themselves.

Some hackers use software to delete other gamers' progress, especially games anyone can host. You might wake up one day and see you've lost your progress.

- Stolen In-game Assets Built Overtime

There are hacks called Trojans; they can record and monitor keyboard strokes. So when a gamer gets hacked by a trojan, it monitors his activities and then analyses the information obtained from the keyboard strokes.

The analyzed data accesses password information the gamers use to unlock their games and access the In-game assets the gamer has amassed over time.

Usually, gamers who have these attacks spend real money to get in-game currencies and then purchase either a new weapon or a new fight suit for their characters that other gamers may not buy because of the cost.

- Cyberbullying and Trolling

Cyberbullying is a vital issue on the list of threats gamers face. Usually, in the spirit of gaming, a player may use a few swear words here and there when he loses or misses a target. Cursing out is understandable, but it becomes an issue when it becomes regular, targeted, and personal.

Games with voice and text features usually have this threat of trolling. Most gamers on these platforms typically abuse these features.

- Fraud

Fraud is a massive problem for gamers. Most times, companies have loopholes in their backend. They may be trying to accommodate the vast influx of gamers into their site and miss out on the minute security details.

Most purchases on game sites need you to input your card details and passwords to complete transactions. Suppose the company pays less attention to its payment gateway and is insecure. Hackers can leverage this and redirect gamers to another site where their card details get stolen.

Now that we have seen how many threats online gamers are against, how much of an issue is it? What do the statistics say?

How Often Do Gaming Cyber Attacks Occur?

A study done by the American content delivery network, Akamai, shows an increase in cyberattacks against game companies by 415 percent in 2018 through 2020.

In a "Gamedemic" report, Akamai made a global report of 6.3 billion cyberattacks, with 4% (246,064,297) of Web attacks targeted at the gaming industry.

Around the world, about 30,000 websites get hacked every day. There is a cyberattack every 39 seconds. And with the present rate, there is an envisaged increase in these attacks and cybercrimes.

This data raises the question, how can you shield yourself from these attackers? What can you do?

How To Protect Yourself From Gaming Cyber Attacks

To mitigate the prevalence of cyber-attacks, you should put security first. You could do this:

- If you get mail or text that you think is suspicious, don't open it or click any link. It might be phishing. Always access your games from the original site.

- If a gamer's comments become offensive or personal, report them to the game moderator. If possible, block them!

- Never reveal sensitive or personal information to your game partners.

- Parents, please encourage your kids to inform you of any cases of bullying or trolling. Teach them never to disclose personal information to strangers.

- Use strong and unique passwords! The importance of strong passwords is worth emphasizing. Don't use easy-to-guess passwords like "1234" or game names or assets in the game you are playing.

- Reject suspicious offers for "freemiums" that seem too good to be true; they probably are.

- As you progress to higher levels in a game, step up your security. Use multiple-factor authentication if available. Be mindful of attempts to steal your identity or information.

Gaming is a thrilling experience! But sometimes, with thrill comes danger. Ensure you put all measures in place to protect yourself and others from gaming attacks.

Reference

https://www.kaspersky.com/blog/online-gamer-threats/4474/amp/

https://www.securitymagazine.com/articles/93764-the-pressures-the-online-gaming-community-faces-when-it-comes-to-cybersecurity

https://cisomag.eccouncil.org/gaming-industry-suffered-12-billion-cyber-attacks-in-past-17-months/amp/

https://www.eset.com/au/about/newsroom/press-releases1/eset-blog/safe-gaming-how-gamers-can-protect-themselves-and-their-pcs-while-playing-online/

https://blog.avast.com/cybersecurity-risks-all-gamers-should-know

https://abcnews.go.com/amp/GMA/Parenting/story?id=5382302&page=1

https://steamcommunity.com/app/218620/discussions/8/619569608735323106/?l=portuguese