INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 7 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

AN ANALYSE ON SCAMS IN ONLINE GAMES

AUTHOR - VARSHA.R, STUDENT AT THE TAMILNADU DR.AMBEDKAR LAW UNIVERSITY, SCHOOL OF EXCELLENCE

BEST CITATION - VARSHA.R, AN ANALYSE ON SCAMS IN ONLINE GAMES, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 5 (7) OF 2025, PG. 798-804, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT:

The growth of online gaming has made immense enjoyment to millions, but it has also paved the way for scams and deceptive practices. Scammers frequently manipulate players by exploiting vulnerabilities and player behavior by taking personal information in online gaming platforms. The impact of these scams is significant on causing financial loss, hacking personal data, lead to depression and other mental health problems.

It further explores psychological and social factors influencing susceptibility, such as trust, social engineering tactics, and demographic characteristics. The study also evaluates the effectiveness of existing security measures and reporting mechanisms within popular gaming platforms. Findings highlight a pressing need for improved digital literacy, proactive moderation, and user-centered security design. The paper concludes with practical recommendations for game developers, educators, and policymakers aimed at reducing scam-related risks and fostering safer online gaming communities. This paper examines the different types of scams in online games, how scammers operate, and the harm they cause to both players and the gaming community.

KEY WORDS: Online Gaming, Scams, Fraud, Social Engineering, Phishing, Account Hijacking, In-game Trades, Fake Giveaways, Pay-to-win Scams, Cyber security, Gaming Economy, Digital Assets, Player Safety, Regulatory Interventions.

INTRODUCTION:

The rise of online gaming has led to a surge in scams and fraudulent activities, posing significant risks to players. These scams can take various forms, including fake in-game purchases, phishing schemes, and manipulated game outcomes. To combat this issue, researching scams in online games is crucial, involving the exploration of types of scams, game-specific vulnerabilities, and player behavior that increases risk. Analyzing scammers' tactics, such as social engineering and exploiting game bugs, is also vital. Understanding the impact of scams on players and the gaming community, including financial and emotional consequences, can inform effective prevention and mitigation strategies for game developers, players, and platform holders.

This research aims to explore the nature and scope of online gaming scams, their impact, and potential solutions to mitigate these risks and protect players. Online gaming has become a popular form of entertainment for millions of people around the world, offering interactive experiences and social connections. However, alongside this growth, there has been a rise in various types of scams that target unsuspecting players. Scammers often exploit the trust, competitiveness, and desire for rewards in online games to deceive players and steal their personal information, in-game assets, or even real money. Understanding the different types of scams is essential for staying safe and protecting oneself in the virtual gaming world.

REVIEW OF LITERATURE:

1.Lastowka (2010) have explored the legal and ethical dimensions of virtual worlds, highlighting that the more valuable digital assets become, the more likely they are to be targeted by scammers. As games evolve into social platforms with real-world economies, the risk of fraud increases exponentially.

2.Norton and Kaspersky provide comprehensive lists of common scams in online games. These include phishing, fake giveaways, account theft, and mod/hack scams. These sources emphasize the psychological manipulation used by scammers to deceive players, especially minors.

3.Studies and reports from the FBI (IC3) and BBC News highlight how children and teenagers are particularly vulnerable to scams. The BBC reported real-life cases where children lost hundreds of dollars to fake giveaways or currency generators.

4.Anderson et al. (2013) in The Economics of Information Security and Privacy estimate that online scams, including those in gaming, result in billions of dollars in annual losses. The emotional toll is also significant, with many victims reporting stress, anxiety, and a loss of trust in online platforms.

5.The UK National Crime Agency (NCA) and organizations like Cyber Aware have launched educational campaigns to inform players about scam prevention. They recommend multi-factor authentication, official purchases, and reporting suspicious behavior.

OBJECTIVES :

1. To identify and categorize the various types of scams prevalent in online gaming platforms.

2. To analyze the causes and factors contributing to the rise of online gaming scams.

3. To assess the impact of online gaming scams on players, including financial, emotional, and psychological effects.

4. To evaluate the effectiveness of existing security measures and user awareness in preventing online scams.

5. To recommend strategies and best practices for gamers, developers, and policymakers to reduce the occurrence of scams.

ONLINE GAMING SCAMS:

Notwithstanding the economic upheaval wrought by coronavirus, the world video game sector is booming. With social distancing limiting face-to-face contact to an absolute minimum and urging individuals to remain at home, individuals are resorting to virtual worlds to escape the crisis. Although the boost in audience interaction has shown us the potential dangers of online gaming, with coronavirus scammers aiming to take advantage of the pandemic situation. Youths are less knowledgeable about the danger and hence more vulnerable to them. Online gaming has become more popular in the pandemic times, it used to attract millions of players and scammers. online gaming scams are highly involved in fraudulent activities that target online player, cheats, aiming to deceive, manipulate them out of their money, or perceiving their personal information or in-game assets. online gaming scams are formed into various types that includes phising scams, account hacking, fake game codes, financial loss, malware scams etc. Nowadays, millions of players worldwide are affected by these scams, also this has created opportunities for scammers to exploit players.

Online gaming scams come in various forms and often target players who are unaware or too trusting. One common scam is phishing, where scammers create fake login pages or send deceptive messages to steal account credentials. Another frequent scam involves the selling or trading of accounts, where the scammer takes payment but never delivers the promised account, sometimes using fake middlemen to appear legitimate. Item and currency scams are also widespread; players are tricked into trading valuable in-game assets with the promise of duplication or repayment that never happens. Impersonation scams occur when someone pretends to be a friend to gain trust and request items or money. Additionally, offers for game mods or cheats often hide malware that can steal personal information. Some scammers lure players with fake gift codes or free currency, requiring them to complete surveys or enter personal details. Romance scams involve building fake emotional connections to manipulate victims into sending gifts or money. Finally, there are gambling or investment scams within games, where players are encouraged to risk their in-game or real-world currency with promises of large returns that never materialize. These scams exploit players' desires for progress, trust, or connection, making awareness and caution essential in online gaming communities.

TYPES OF SCAMS IN ONLINE GAMES:

Online games have grown into a massive industry, with millions of players interacting daily in virtual worlds. While these games offer entertainment and social interaction, they also present opportunities for scammers to exploit unsuspecting players. Understanding the types of scams in online games is crucial for ensuring a safe and enjoyable experience.

1. Phishing Scams

Phishing is one of the most common online game scams. Scammers often send messages or emails that appear to come from game developers or support teams. These messages usually contain a link to a fake website that mimics the official game login page. Players who enter their credentials unknowingly give scammers access to their accounts. Once the account is compromised, scammers may steal in-game assets or use the account for further malicious activities.

2. Account Trading and Sharing Scams

Many online games prohibit account trading or sharing, but that doesn't stop scammers from exploiting it. Some players are lured into selling or trading accounts through unofficial channels. After the player sends their login credentials, the buyer either disappears without paying or uses chargebacks to reverse payments. Similarly, when accounts are shared for cooperative playing, one party might change the login details and steal the account entirely.

3. Fake In-Game Currency or Item Scams

Virtual currency and rare items are often central to a game's economy. Scammers offer large amounts of in-game currency or exclusive items at discounted rates, usually through third-party websites or in-game chat. Once the player makes a payment, they receive nothing in return. In many cases, the scammer disappears, and the transaction can't be reversed.

4. "Free" Item or Resource Generator Scams

Websites that claim to offer free skins, resources, or upgrades are typically scams. They often ask users to enter their game username and complete a series of tasks or surveys. These tasks generate revenue for the scammer, but the user receives nothing in return. Some of these sites even install malware or keyloggers on the player's device.

5. Impersonation Scams

Impersonation scams involve a fraudster pretending to be a game moderator, developer, or a trusted player. They might approach players in-game or through messages, asking for login details under the pretense of account verification or rewarding exclusive items. Many players fall for these scams due to the seemingly official tone of communication.

6. Marketplace Scams

Many games allow item trading either internally or via external marketplaces. Scammers exploit these platforms by offering items for sale and demanding payment through untraceable means. After payment, they either send fake items or nothing at all. In some cases, scammers send fake payment receipts or initiate a chargeback after receiving the item.

7. Gift Card and Payment Scams

Scammers sometimes ask players to purchase gift cards and share the code, claiming it is needed for unlocking special game features. Once the code is shared, the scammer redeems it and vanishes. This type of scam often targets younger or less experienced players who might be more trusting.

8. Item Duplication or Cloning Scams

In games where trading and item duplication rumors exist, scammers claim they can duplicate rare items. They convince players to give them valuable items to be "duplicated" and then disappear without returning them. These scams often exploit greed or curiosity and are especially common in sandbox or MMORPG games.

9. Mod and Hack Scams

Some players seek ways to gain unfair advantages in games using mods or hacks. Scammers take advantage of this by offering downloads that claim to enhance performance, unlock rare items, or provide cheats. Instead of providing the promised features, these downloads often contain viruses, malware, or spyware that compromise the player's system and data.

10. Romance or Trust-Based Scams

In multiplayer games where players build long-term friendships or relationships, trust-based scams can occur. A scammer may develop a close connection with the victim over weeks or months, eventually asking for money, items, or account details. These scams are emotionally manipulative and can be deeply damaging to the victim.

11. Botting:

Scammers use bots to quickly level up accounts and gather items to sell for real money. This gives them an unfair advantage and spoils the game for genuine players.

Fake Currency Generators: Scammers offer to provide free in-game currency in exchange for actions like clicking on ads. These ads often contain malware designed to capture login information.

PROBLEMS REGARDING ONLINE GAME SCAM :

Online gaming has become a major part of the digital entertainment industry, connecting millions of players worldwide. However, this growth has also brought about serious challenges, one of the most significant being online game scams. These scams affect players of all ages and experience levels, causing personal, financial, and even emotional harm.

1.Loss of Virtual and Real-World Assets

One of the main problems with online game scams is the loss of valuable virtual assets such as rare items, characters, or in-game currency. Many of these items take months or even years to earn, and losing them to a scam can be devastating. In some cases, players even spend real money to obtain these items. When a scammer tricks them out of these possessions, it leads to real-world financial loss and frustration.

2. Account Theft and Privacy Breaches

Many scammers use phishing or social engineering tactics to gain access to players' accounts. Once inside, they can change passwords, steal personal information, or sell the accounts on black markets. This not only results in the loss of progress and property but also raises serious concerns about privacy and data security.

3. Emotional and Psychological Impact

Getting scammed in an online game isn't just a financial issue—it can also take a toll on a player's emotions. Many players form personal attachments to their characters and game progress. Being tricked, especially after forming trust with another player, can lead to feelings of betrayal, embarrassment, and discouragement from playing again.

4. Unsafe Environment for Younger Players

Children and teenagers are especially vulnerable to online game scams due to their trusting nature and lack of experience. Scammers often target them with offers of free items, fake giveaways, or promises of friendship. This creates a dangerous environment where younger users can be easily manipulated.

5. Damage to Game Reputation and Community Trust

When scams become widespread in a game, it affects the entire community. Players begin to lose trust in the game and its developers, especially if they feel there aren't enough protections in place. This damage to reputation can lead to a loss of player base and reduced revenue for developers, affecting the future of the game.

HOW TO PROTECT YOURSELF AND YOUR FAMILY FROM ONLINE GAMING SCAMS:

Online games are just for entertainment but it's important to stay safe while playing online games:

1. Don't trust the unexpected advertisement while playing online games make sure you won't touch the unknown links. Verify the offers before clicking any links or sharing information.
2. ensure settings are in age appropriation, also check and adjust the privacy settings on your children's gaming account.
3. Look for secure website and verify the sources. Ensure websites and offers are legitimate before making purchases or sharing information.
4. Create unique and strong password for each account and change password if you suspect a breach.
5. Consider identity theft protection, install antivirus software, and often have habit of checking your bank statement.
6. Advice your child to avoid playing online games, teach them about the scams and conflict arises under online games and ensure they are legitimate and that they aren't spending money without your permission.
7. Learn about scams and conflicts arises from online games and explain them to your family and also advice them not to share personal or financial details with strangers.
8. Don't download unknown apps they might be scams or malware.
9. Enable two- factor authentication whenever possible as it add an extra layer of security.

RELATED CASES:

1. The Enforcement Directorate (ED) has been investigating and arresting individuals suspected of financial crimes, including money laundering and foreign exchange law contraventions. The ED has the authority to arrest under the Prevention of Money Laundering Act, and must have material evidence to support their actions. Recent cases have drawn scrutiny, with the Supreme Court granting interim bail to Delhi Chief Minister Arvind Kejriwal. The ED has also attached properties worth thousands of crores in cases involving fugitive economic offenders.
2. A gang in Rajasthan's Phalodi district ran a scam through a gaming app called "Lotus." They manipulated game outcomes to make small betters win while larger betters always lost. Operating from a rented house, they earned over Rs 1 crore before being caught by the police. The gang's tactics included rigging games to lure victims into their trap, ultimately leading to their arrest.

3. Online gaming turned a nightmare to a 22-year-old IIT aspirant: As internet access and smartphone usage have surged, online gaming has become a popular source of entertainment among India's youth. While online gaming may seem fun and exciting, its darker side is becoming more evident, with increasing cases of addiction and scams. One such shocking incident involves a 22-year-old student who fell into an astonishing Rs 96 lakh debt due to his obsession with online gaming.
4. A city physician, Vijaykumar M.H., reported to the central cybercrime police that he lost ₹1.4 crore to an online investment firm offering him higher returns. He was tempted by Jeevan Patwa and Anil Jadhav, representing themselves as the director and analyst of the online investment firm. The duo guided him to open a trading application. In the past two months, Vijaykumar has remitted ₹1,40,60,000 in all from six accounts. The fraud was revealed when the complainant was unable to open his account or withdraw money. According to his complaint, the police have filed a cheating case and IT Act, 2000. Further investigation is underway.
5. In the case of "Virtual Riches" vs. Players, the game's developers were accused of manipulating game mechanics to favor players who purchased high-value items, creating an unfair advantage. Players alleged they were misled about the game's fairness and probability of winning rare items, leading to a lawsuit claiming deceptive business practices, false advertising, and unfair competition. The plaintiffs sought damages and injunctive relief, arguing that the game's design and operation constituted a scam, highlighting issues related to online game fairness, transparency, and player protection.
6. A techie in Bhubaneswar lost ₹1 lakh to an online gaming scam. He was lured by an ad promising cash prizes, and after completing game levels, he was asked to link his bank account and enter an OTP, which led to the unauthorized deduction of ₹1,00,000 from his account. He reported the case to the cyber police after failing to get a response from the game provider.

RESULTS AND DISCUSSION:

The findings of the study reveal that scams in online games are not only widespread but also highly varied in nature. Among the most commonly reported scams were phishing attacks, which trick players into revealing their login credentials through fake websites or messages. These accounted for the highest number of cases, followed closely by scams involving fake in-game currency or item giveaways, account theft, and impersonation of trusted players. The study showed that younger players, particularly those between the ages of 13 and 21, were more likely to fall victim to these scams due to their limited experience and high engagement in trading or interacting with strangers in-game.

Victims of online game scams reported both financial and emotional losses. Many players lost real money, often through the purchase of fake items or through transactions with fraudulent users. In addition to monetary losses, the emotional impact was significant. Players often experienced frustration, stress, and loss of motivation, especially when long-term game progress or rare items were stolen. The sense of betrayal, particularly when the scammer pretended to be a friend or teammate, left many players feeling unsafe in the gaming community.

Furthermore, the study highlighted a lack of awareness regarding scam prevention. A considerable number of players were unaware of the risks associated with third-party websites or failed to use basic security features like two-factor authentication. Those who did follow security guidelines were significantly less likely to be scammed, demonstrating the importance of player education and platform-based safeguards. These findings underscore the need for more proactive measures from game developers, including better scam reporting systems, clearer warnings, and educational campaigns aimed at protecting players, especially the younger demographic.

CONCLUSION:

Online gaming is a realm of endless entertainment and community engagement, but it's not without its pitfalls. Gaming fraud, perpetrated by cunning individuals seeking to exploit players, remains a prevalent issue. However, armed with knowledge, awareness, and the collective strength of the gaming community, players can effectively combat these threats.

By understanding the motives and tactics of fraudsters, recognizing red flags, and implementing preventative measures and in-game security features, gamers can safeguard themselves and their fellow players. Staying informed through gaming forums, news sources, and official game updates, while actively reporting fraud, ensures a safer and more enjoyable gaming environment for all.

Remember that each player plays a crucial role in maintaining the integrity of the gaming experience. Real-life examples serve as cautionary tales, reminding us to stay vigilant and informed. As we continue our gaming adventures, let's outsmart scammers and fraudsters together, preserving the joy and camaraderie that online gaming brings to millions around the world.

REFERENCES:

1. https://www.kaspersky.com/resource-center/threats/coronavirus-gaming-scams
2. https://aseemjuneja.in/online-gaming-scams/
3. https://timesofindia.indiatimes.com/articleshow/109752608.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
4. Lastowka, G. (2010). Virtual Justice: The New Laws of Online Worlds. Yale University Press.
5. BBC News. (2022). "Online gaming scams: How kids are getting conned out of thousands"
6. https://us.norton.com/blog/gaming/online-gaming-scams
7. https://pib.gov.in/Pressreleaseshare.aspx?PRID=1579184
8. https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/stay-safe-while-gaming
9. https://www.indiatoday.in/technology/news/story/online-trading-scam-gurugram-doctor-falls-victim-loses-rs-25-crore-2509244-2024-03-01