OXFORD JOURNAL
OF STUDENT
SCHOLARSHIP

Security Issues in Online Gaming: Its Causes and Its Possible Solutions

Anvit Ashok Limbekar
anvit.limbekar@gmail.com

ABSTRACT

The rapid growth of online gaming has made it one of the largest digital entertainment industries in the world, but also increased its exposure to cybersecurity threats. In this paper, we have performed an exhaustive analysis of the main causes of cybersecurity problems in online gaming, studied the most important security threats faced by players and gaming platforms, and evaluated the existing and emerging mitigation strategies. The results highlight the key drivers of cybersecurity risks as digital illiteracy, economic value of digital assets, weak regulatory frameworks, security-performance trade-offs and gaming black markets. The study also analyses game server exploits, Distributed Denial-of-Service (DDoS) attacks, phishing and social engineering, malware and cheat-driven infections and privacy and behavioural exploitation, highlighting their technical characteristics, impacts and long-term challenges. Comparison of the existing solutions shows that there is no single approach that is enough. But the best way to improve the security, resilience and sustainability of online gaming ecosystems is through a combination of technical safeguards, cybersecurity awareness, industry cooperation, regulatory measures and emerging technologies.

Keywords*:* Online Gaming Security, Cyberattacks, Data Privacy, Phishing, Distributed Denial of Service (DDoS), Malware, Multi-Factor Authentication (MFA), Virtual Economies, Digital Illiteracy

METHODOLOGY

In this study, a qualitative narrative literature review was conducted to identify the main cybersecurity issues in online gaming and the mitigation strategies. To identify relevant literature, we performed a systematic search of established academic databases that provide comprehensive coverage of cybersecurity, computer science, information security, and online gaming research. The review is based mainly on the peer-reviewed journal articles, conference proceedings and recognised academic publications published between 2018 and 2026. In order to increase the reliability, credibility and completeness of the review, priority was given to literature published in high-quality peer-reviewed journals with strong academic impact. Earlier publications were only included if they introduced fundamental concepts or important regulatory frameworks that are essential to understand the topic, such

as the General Data Protection Regulation (GDPR). The review excluded articles that lacked sufficient academic credibility, duplicate studies, articles published in a non-English language, opinion articles, and studies that are unrelated to cybersecurity in online gaming. Thirty relevant references were identified for detailed analysis after screening. Instead of a statistical meta-analysis, this study used a qualitative comparative thematic analysis to synthesise and critically appraise the selected literature. The analysis was performed on three main components of the study: The causes of cybersecurity issues were analysed by identifying each underlying cause, explaining why it occurs, examining how it contributes to cybersecurity risks within online gaming, evaluating its impact on players and the gaming ecosystem and assessing the relationships between the different contributing factors. Security issues were analysed by examining the characteristics and technical mechanisms of each threat, identifying why players and gaming platforms are vulnerable, determining the most affected gaming platforms, evaluating user, financial, operational and ecosystem impacts, assessing why existing cybersecurity measures remain insufficient and discussing long-term and emerging cybersecurity challenges associated with each threat. Possible solutions were analysed by describing how each mitigation strategy works, identifying the cybersecurity issues and root causes it addresses, evaluating its practicality and implementation challenges, assessing its effectiveness in mitigating cybersecurity risks, and examining its impact on gameplay performance and user experience, as well as its long-term applicability within online gaming environments. Finally, comparative tables were created to systematically compare the identified causes, security issues, gaming platforms, and cybersecurity solutions in terms of their characteristics, severity, implementation considerations, practicality, effectiveness, and overall impact. This comparative approach provides a structured synthesis of the literature, allowing for a clearer assessment of the relationships between cybersecurity threats and their corresponding mitigation strategies.

INTRODUCTION

The size of online gaming has increased massively, making it one of the world's largest digital entertainment industries, connecting millions of players through multiplayer platforms, virtual economies and cloud-based services. Although these developments have improved user experience and accessibility, they have also increased the cybersecurity attack surface, leaving players and gaming platforms vulnerable to ever more sophisticated cyber threats (1).

Unlike traditional single-player games, online gaming involves constant exchange of personal information, digital assets and financial transactions, making it vulnerable to phishing, malware, Distributed Denial-of-Service (DDoS) attacks, account compromise and privacy breaches. While individual cybersecurity threats have been studied, a comprehensive understanding of their root causes and corresponding mitigation strategies is missing. This literature review therefore reviews the causes of cybersecurity issues in online gaming, analyses major cybersecurity threats and evaluates existing and emerging approaches for improving cybersecurity within the gaming ecosystem.

CAUSES OF DATA SECURITY ISSUES:

(1) Digital Illiteracy

One of the main human factors that leads to cybersecurity vulnerabilities in online gaming is digital illiteracy. It is not only the lack of ability to use digital technologies, but also the lack of awareness to identify cyber threats, to assess the authenticity of online interactions and to participate online safely. Thus, players with low digital literacy are more prone to share personal information, use weak passwords, click suspicious links, or download from untrusted sources, increasing the risk of phishing attacks, malware infections, account hijacking, and identity theft (2).

Online games are interactive, and this is particularly worrying for digital illiteracy. In multiplayer games, players have to communicate all the time via voice and text chat when working with teammates, friends and strangers alike. In the course of such interactions, players may unintentionally disclose sensitive information like email addresses, phone numbers or social media accounts. Cybercriminals often abuse this trust by pretending to be teammates, experienced players, or game administrators to do phishing attacks and other social engineering techniques. Similarly, many players download unofficial modifications (mods), cheats or cracked versions of games from untrusted websites without checking their authenticity. These downloads may contain malware, spyware, ransomware or credential-stealing software disguised as legitimate gaming content. Such behaviours demonstrate how a low level of digital awareness provides attackers with ample opportunities to attack users.

The link between digital literacy and cybersecurity awareness is strongly supported by recent peer-reviewed research. Those with higher digital literacy levels are more likely to adopt safe online behaviours such as enabling multi-factor authentication, using strong passwords, spotting phishing attempts, and updating security software regularly. By contrast, users with limited knowledge of cybersecurity are much more likely to engage in unsafe online behaviours that increase the chances of credential theft, malware infections and social engineering attacks. Moreover, human-centred cybersecurity studies further emphasise that user behaviour is still one of the most significant contributors to cybersecurity incidents and that digital literacy is a critical factor in reducing human-related security risks (3).

The ramifications of digital illiteracy are not limited to individual players but affect the entire online gaming ecosystem. If the gamers are not aware of cybersecurity, they become more susceptible to phishing, malware, account theft, and identity fraud. This expands the attack surface of the gaming platforms. Such events may lead to a surge in account recovery requests, financial losses due to fraudulent transactions, increased operational costs for developers and a

decrease in the trust of gaming communities. Similarly, in competitive gaming, compromised accounts and stolen digital assets can undermine fair play and negatively impact player retention and platform reputation.

Digital illiteracy is much more widespread than most technical vulnerabilities. It allows all sorts of cyber attacks, not just a single exploit. Because of software vulnerabilities or server misconfiguration, often only a part of a gaming platform is affected. Digital illiteracy, in turn, influences users' decisions about an array of online activities, from talking to others and managing accounts to downloading files and protecting privacy. It doesn't create a single security hole, but it does make a lot of attack vectors more effective, which adds to cybersecurity risk on a fundamental level.

(2) Economic value for the digital assets

The shift to online gaming has meant virtual items are worth something in the real world, not just in-game rewards. Today's games are built around complex virtual economies where players buy, earn, trade and sell digital assets such as weapon skins, character costumes, virtual currencies, collectibles and premium accounts. With the rise of microtransactions and player-created marketplaces, the monetary value of these assets has skyrocketed, with some rare items going for hundreds or thousands of dollars. Gaming accounts are, therefore, not only a source of entertainment but also valuable digital assets and attractive targets for financially motivated cybercriminals (4).

The high monetary value of digital assets has changed the motivations for cyber attacks on online games fundamentally. This is a shift away from hackers simply wanting to break the game to make some cash by hacking gaming accounts that have valuable virtual items or payment details on them. They use different methods, including phishing attacks, stealing credentials, distributing malware, social engineering and fake trading schemes, to gain access to these assets without authorisation. Attackers can convert virtual assets into real-world financial gains by utilising illicit online marketplaces to trade stolen virtual goods and compromised accounts. This exponential growth of virtual economies has spawned lucrative opportunities for organised cybercrime (5).

Peer-reviewed research has found that virtual asset marketplaces have become an increasingly important element of cybercriminal activity, providing convenient avenues for illicit proceeds to flow in and out of online gaming ecosystems. With the rise of microtransactions, virtual marketplaces and player-to-player trading, the possibility of account theft, virtual asset fraud, and unauthorised trading of digital goods has become a reality. As the size of virtual economies increases, cyber criminals are moving their focus from exploiting technical vulnerabilities to the huge financial value embedded in gaming platforms. These findings highlight the economic incentive as a key driver of cybersecurity threats in the modern online gaming ecosystem (5).

The trend has implications that go beyond the individual monetary losses players experience. For example, a successful theft of valuable digital assets could result in loss of confidence by players, additional costs to developers in terms of customer support and account recovery, disruption of virtual economies and growth of illicit trading markets. The commercialisation of digital assets also increases the costs for game developers to fight fraud, can harm their reputation and affects the stability of virtual economies that rely on fair and secure in-game transactions.

Virtual goods are of ever-increasing economic value and therefore an increasingly attractive target for organised cyber-criminals. The growing digital illiteracy, coupled with the financial value of digital assets, makes online gaming platforms a lucrative target for cyber criminals. As virtual economies grow and digital assets become more valuable, financially motivated cyberattacks are likely to become more frequent and sophisticated. This way, the commodification of virtual assets has become one of the main drivers of cybercrime in the modern online gaming ecosystem.

(3) Weak Regulatory Frameworks

The rapid growth of online gaming has left behind the development of a full set of cybersecurity regulations, leaving players with patchy legal protections across different jurisdictions. The online gaming industry is distinct from other industries like banking and healthcare, which are generally governed by existing cybersecurity and data protection laws. In the online gaming industry, cybersecurity requirements, data protection obligations and enforcement differ significantly from one country to another. The European Union's General Data Protection Regulation (GDPR) has set a high standard for personal data protection and organisational accountability, but there are no such regulatory standards that have been adopted globally. These inconsistencies result in regulatory gaps that could diminish the overall security and privacy of globally connected gaming platforms (6).

Without harmonised international regulations, it is becoming increasingly difficult for gaming companies to apply uniform cybersecurity practices across platforms that cater to millions of users worldwide. Different cybersecurity laws, data protection requirements, incident notification duties and legal procedures in different countries often make security incident management a complicated issue. Cross-border cyberattacks frequently cross multiple jurisdictions, making it much harder to attribute, investigate and prosecute offenders. Differences between legal systems, requirements for digital evidence and mechanisms for international cooperation all contribute to this difficulty (7). So, the legal and procedural complexities can be abused by attackers, while gaming companies face significant operational and legal challenges in responding to cross-border cybersecurity incidents.

A recent research on cybersecurity points out the persistent challenge of regulatory fragmentation for the safeguarding of digitally interconnected global ecosystems. The lack of globally coordinated cybersecurity policies can hinder incident response, complicate the sharing of digital evidence, and diminish the effectiveness of law enforcement agencies in cross-border cybercrime investigations (7). These challenges are particularly relevant in the online gaming space, as the major gaming platforms handle large volumes of personal, financial and transactional data of players from many countries at the same time. Consistent regulatory oversight becomes more and more important.

Weak regulatory frameworks have implications beyond legal compliance. Uneven rules could lead to uneven levels of cybersecurity, uneven levels of player privacy protection, and delays in responding to security incidents. Simultaneously, developers have to comply with a number of regulatory regimes across jurisdictions, which adds to operational complexity and compliance costs, and makes it more difficult to maintain uniform security practices. These limitations could eventually undermine user trust and decrease the overall resilience of online gaming ecosystems in the face of evolving cyber threats. These challenges affect multiple stakeholders, including regulatory authorities responsible for enforcing cybersecurity legislation, developers required to comply with differing legal requirements, and users who may receive inconsistent levels of legal protection across jurisdictions.

This is unlike digital illiteracy that mainly exposes users to cyberattacks and the economic value of digital assets that provide financial incentives for attackers. Weak regulatory frameworks affect the general environment within which cybersecurity is managed. They do not themselves generate technical vulnerabilities, but they undermine the effectiveness of prevention, investigation and legal enforcement by allowing inconsistencies between national regulatory systems to persist. They do not create technical vulnerabilities as such, but they undermine the effectiveness of prevention, investigation and legal enforcement by allowing inconsistencies to live on between national regulatory systems.

(4) Security vs Performance Trade-offs

One of the most important technical challenges of modern online gaming today is to keep a good balance between cybersecurity and gameplay performance. Unlike most digital applications, online multiplayer games require low latency, real-time synchronization and continuous communication to provide a smooth gameplay. Any lag in data transfer or processing, even in a range of milliseconds, can be very detrimental to the gameplay, especially in a competitive environment where a range of milliseconds can determine the performance of a player. So developers need to build in strong security without sacrificing the responsiveness and fluidity players expect. (8) This balance is crucial for both system security and user satisfaction.

Many security mechanisms (e.g., encryption, server-side validation, more sophisticated anti-cheat systems, strong authentication protocols) lead to computational or communication overhead that should be carefully handled to preserve gameplay performance. These mechanisms are important to prevent unauthorised access, cheating, data manipulation and other cyber threats, but inefficient implementation can lead to an increase in network latency, server load or authentication time (8).

Research shows that security-performance tradeoffs are still a challenge in designing online gaming systems. Inadequate or poorly implemented security controls can leave gaming platforms vulnerable to account takeover, unauthorised access, cheating and data tampering. However, too much security overhead can hurt responsiveness, resource consumption and player engagement (8).

This trade-off does not only have implications for the design of technical systems. Poor security implementations can result in loss of money, compromised player accounts, damage to reputation and loss of user trust. Overly restrictive security measures can frustrate players through increased loading times, authentication delays or network lag. Therefore, the security-performance trade-off directly impacts the technical reliability of gaming platforms and the quality of the player experience, representing a persistent challenge in modern online game development.

While the lack of digital literacy simply augments the vulnerability of users to cyberattacks, and weak regulatory frameworks dictate the governance and enforcement of cybersecurity, security-performance trade-offs result from technical design choices made during the development of gaming systems. Security-performance trade-offs stem from the technical choices made in the design and development of gaming systems. Given the complexity of the development of multiplayer infrastructures and the size of the player community in online games, a reasonable compromise between cybersecurity and performance has become a requirement for secure, reliable and engaging online gaming ecosystems.

(5) Increase in the Gaming black market

As online gaming commercialises, black markets for the trade of gaming accounts, game currency and other digital items outside official channels are emerging. These black markets largely operate based on Real Money Trading (RMT), where virtual assets are traded for real-world currency without the consent of the game developers. The value of virtual assets has increased, and these underground economies have flourished. Illicit trade has shifted from a series of ad hoc transactions to organised markets with buyers and professional sellers (9).

These underground marketplaces offer a profitable financial incentive for cybercriminals to obtain high-value gaming assets via illicit means. A cyberattack can also be lucrative for the attacker, who can sell the hacked gaming account, rare virtual items or in-game currencies on

black-market platforms. Further research shows that these markets are increasingly dominated by professional vendors who use organised trading networks to increase the efficiency and scale of illicit transactions. Underground trading is a lucrative business, and online gaming platforms and users are under constant attack (9).

The studies also show that the black markets have been transformed from informal exchanges between individual actors into more and more organised economic systems. Network analysis indicates that some large trading groups dominate large segments of the illicit market and that there is a trend towards increasing professionalisation of unauthorised virtual asset trading. This evolution makes underground markets more resilient and difficult for developers to detect and disrupt (9).

However, these underground economies have implications beyond the monetary losses of individual players. The illegal trade of virtual assets can hurt the players' confidence, destabilise the game economy, harm the reputation of gaming companies and undermine the success of legal monetisation systems. Developers also have to spend more on monitoring suspicious transactions, recovering compromised accounts and enforcing policies against unauthorised trading. Consequently, the effects of gaming black markets extend beyond individual victims to influence developers, legitimate virtual economies, platform security, and the overall integrity of the online gaming ecosystem.

The economic value of digital assets is the monetary incentive for cybercrime. Stolen virtual goods and hacked accounts are converted into cash in the gaming black markets. These underground marketplaces provide a formalised venue for the exchange of illicit gaming assets, and are vital to the viability and profitability of cybercrime within the online gaming ecosystem.

Table 1. Comparative Analysis of the Causes of Cybersecurity Issues in Online Gaming				
Cause	**Primary Contribution to Cybersecurity Issues**	**Frequency in Literature**	**Scope of Influence**	**Overall Risk Level**
Digital Illiteracy	Increases users' susceptibility to cyber threats through poor cybersecurity awareness and unsafe online behaviour.	High	Individual users	High
Economic Value of Digital Assets	Creates financial incentives for cybercriminals by assigning real-world value to gaming accounts, virtual currencies, and digital assets.	High	Users, developers, and virtual economies	Very High
Weak Regulatory Frameworks	Restricts effective governance, legal enforcement, and international cooperation against cybercrime.	Moderate	Gaming industry and regulatory authorities	High
Security–Performanc e Trade-offs	Requires developers to balance robust security mechanisms with low latency and gameplay performance, potentially creating exploitable vulnerabilities.	Moderate	Game developers and gaming platforms	Moderate-High
Growth of the Gaming Black Market	Facilitates the commercialisation of stolen accounts and virtual assets through organised underground trading networks.	Moderate	Entire online gaming ecosystem	High
Sources: ***Authors' synthesis based on the reviewed literature (3, 4, 6, 8, 9).***				

Cybersecurity issues in online gaming arise from a variety of interconnected factors affecting different elements of the gaming ecosystem, as illustrated in **Table 1**. The economic value of digital assets is the single biggest overall risk, because it is the main financial motivator of cybercrime activity. On the other hand, digital illiteracy continues to be a significant human factor that increases users' vulnerability to cyber threats, while weak regulatory frameworks hinder effective legal enforcement and international cooperation. Security–performance trade-offs, unlike the other causes, are due to the technical design decisions, where the developers have to balance between strong security and gameplay performance. Meanwhile, the growth of the gaming black market fuels cybercrime by facilitating the commodification of stolen digital assets. Taken together, these findings suggest that the cybersecurity challenges in online gaming are the result of the interaction of human, economic, technical, regulatory and criminal ecosystem factors, and that mitigation strategies must therefore be comprehensive and coordinated.

SECURITY ISSUES IN ONLINE GAMING:

(1) Game server exploits

Game server exploits are attacks on the infrastructure that handles player authentication, matchmaking, game state synchronisation and persistent player data. Attackers take advantage of weaknesses in server infrastructure, network protocols, or server-side logic to manipulate gameplay, gain an unfair competitive advantage, disrupt online services, or access sensitive player information. Modern networked games use authoritative server models extensively to ensure game integrity. In such models all important game decisions are made by centralized servers and not by players themselves. However, this centralisation also means that a single vulnerability on the server side can affect all connected players at the same time. Online gamers are particularly vulnerable as they have little direct control over server security (8). Buffer overflow attacks take advantage of vulnerabilities in the way software handles memory, allowing the execution of malicious code or the compromise of server processes. Distributed Denial-of-Service (DDoS) attacks aim to flood a server with an overwhelming amount of network traffic, or synchronised requests at the application layer. Recent studies have also shown that application-layer DDoS attacks in massively multiplayer online (MMO) games can generate legitimate-looking in-game interactions that significantly degrade server performance, while being difficult to distinguish from normal player behaviour (10).

A successful server compromise can have much broader impact than a simple temporary service outage, as game servers represent the authoritative backbone of modern online gaming ecosystems. A single infrastructure vulnerability can simultaneously compromise service availability, gameplay fairness, state synchronization, and player trust, leading to financial losses, reputational damage, increased operational costs associated with incident response and account recovery, and long-term reductions in player retention. This is particularly true for massively multiplayer online (MMO), cloud and live-service games, which rely on centralised servers to

provide persistent virtual worlds and millions of real-time interactions. Games that are played offline and peer-to-peer tend to have less centralized attack surfaces and therefore are relatively less vulnerable to this kind of threat. Phishing attacks target individual users, but game server exploits threaten the entire gaming platform. A single compromised vulnerability can impact millions of players at the same time, disrupting competitive tournaments, virtual economies and community confidence. Existing security measures are often not enough because developers have to constantly find a compromise between strong server-side protection and low-latency gameplay. Frequent software updates, increasing game functionality and ever complex networking architectures constantly provide new opportunities for attacks. Recent research among professional game developers also shows that persistent server-side vulnerabilities often result from limited security expertise, poor security testing and compressed development schedules (11). As online gaming continues its natural evolution to cloud-based infrastructures, cross-platform ecosystems, and ever more persistent virtual worlds, the maintenance of secure server architectures without compromising gameplay performance will remain one of the most significant long-term cybersecurity challenges facing the gaming industry.

(2) Distributed Denial of Service (DDoS) attacks

One of the most disruptive cybersecurity threats to online gaming is the **Distributed Denial-of-Service (DDoS)** attack. Unlike many other cyberattacks, DDoS attacks do not directly compromise sensitive data but instead target the continuous availability of gaming services. A DDoS attack involves using numerous compromised devices, commonly organised into botnets, to flood a gaming server with overwhelming volumes of malicious network traffic or application-layer requests. This exhausts the server's computational and networking resources, preventing legitimate players from accessing online services. Because these attacks originate from multiple distributed sources, they are significantly more difficult to detect and mitigate than conventional Denial-of-Service (DoS) attacks. Recent research has also shown that application-layer DDoS attacks can exploit legitimate in-game interactions, allowing attackers to degrade server performance while remaining difficult to distinguish from normal player behaviour (10). Since online gamers rely on uninterrupted server connectivity for matchmaking, real-time communication and game state synchronisation, even a temporary service disruption can immediately prevent legitimate users from participating, despite their own devices remaining uncompromised.

The impact of DDoS attacks extends far beyond temporary gameplay interruptions. High latency, server disconnections and prolonged service outages reduce player satisfaction, disrupt competitive matches and can result in significant financial losses for game developers, esports organisers and professional players competing in prize tournaments. Extended outages may also increase customer support costs, reduce player retention and damage the long-term reputation of gaming platforms. These consequences are particularly severe for cloud-based, live-service and massively multiplayer online (MMO) games, where persistent connectivity and low-latency

communication are fundamental to gameplay, whereas offline games experience comparatively limited exposure because they do not rely on continuously available online infrastructure. DDoS attacks are designed to exhaust server resources until legitimate users can no longer access the service, rather than compromising the integrity of stored data or software. Existing defensive mechanisms are becoming progressively less effective because modern botnets generate highly distributed traffic patterns that closely resemble legitimate user behaviour, allowing malicious traffic to evade traditional filtering and detection systems (12). As cloud gaming, large-scale multiplayer ecosystems and global esports continue to expand, defending against increasingly sophisticated, adaptive and large-scale DDoS attacks while maintaining uninterrupted gameplay will remain one of the major long-term cybersecurity challenges for the online gaming industry.

(3) Phishing and Social Engineering

Phishing and social engineering are two of the most prevalent cybersecurity threats in online gaming. Unlike many other cyberattacks these threats exploit human behaviour rather than technical vulnerabilities. Instead of targeting gaming infrastructure directly, cybercriminals employ social engineering to trick players into voluntarily providing sensitive information, including login credentials, payment information or authentication codes. Common tactics include: email messages with fake sender addresses, fake gaming Web sites, fake tournament invitations, malicious links sent through in-game chat or messaging services, impersonating game administrators or trusted members of the community. Recent systematic reviews have pointed to the increasing combination of technical deception and psychological manipulation in modern phishing campaigns, where attackers exploit trust, urgency, authority and attractive rewards to maximise the likelihood of success (13,14). Players tend to interact with strangers, join online communities and exchange digital content during the game play. Players, therefore, are particularly vulnerable to social engineering tricks that exploit regular social interactions, rather than vulnerabilities in computer systems.

Phishing attacks are a lot more than just account stealing. Accounts for gaming are lucrative targets for financial fraud, identity theft, and other cyberattacks because they typically contain valuable in-game items, connected payment methods, personal information, and years of progress in a game. Apart from immediate financial losses, compromised accounts can result in permanent loss of digital assets, reputational damage within gaming communities and reduced trust in online gaming platforms. Unlike game server exploits or Distributed Denial-of-Service (DDoS) attacks, which target gaming infrastructure, phishing attacks rely on human judgement, not software flaws, so the main defence is user awareness. MMO (Massively Multiplayer Online) games, esports communities, live-streaming platforms and gaming social media are especially vulnerable, because players constantly interact and attackers can build trust before running scams. Although technical security measures are constantly being improved, phishing is difficult to eradicate because attackers rapidly modify their methods, exploit the lack of cybersecurity awareness and exploit the poor verification of online communications (13,14). With online gaming becoming

more and more connected through cross-platform ecosystems, live-streaming services and growing social features, separating the real communications from the increasingly sophisticated phishing attempts will remain a major long-term cybersecurity challenge.

(4) Malware and cheat-driven infection

Malware and cheat-driven infection This is when malicious software is bundled with unofficial game modifications, cheat programs, cracked game files and other untrusted third-party downloads. These apps often tout unfair in-game advantages, free digital goods, or better performance, tempting users to install software from unknown sources. Once running, the malware can download trojans, spyware, credential stealers, remote-access tools or other malicious components that allow attackers to maintain persistent access to the victim's device while remaining difficult to detect. Due to the highly competitive nature of online gaming, some players opt for the short-term gains of in-game advantages over cybersecurity risks. Hence, cheat software and unofficial downloads are attractive routes for malware distribution. Cheating in online games is a well-studied problem and cheat programs usually require deep interaction with game processes and system memory, which grants elevated privileges to untrusted software and creates additional chances for malicious exploitation (15). Moreover, recent studies have shown that unofficial and pirated software downloaded from untrusted online sources are often used to hide malware that can install Trojans, adware, malicious backdoors and other persistent threats that jeopardize system security (16). These programs often seem to offer appealing gaming benefits , so players may unknowingly bypass security measures , which can result in increased exposure to malware infections .

The consequences reach much further than just unfair play. Malware can provide continuous monitoring of user activity, steal gaming credentials, compromise linked payment methods, create malicious backdoors, and provide attackers with persistent remote access to compromised systems (16). Phishing is when users are deceived into voluntarily giving sensitive information. Malware, when installed, automatically gathers, transmits and exploits data often with no further user input needed. PC gaming platforms are particularly vulnerable due to the wide support for game modifications, executable downloads and an active third-party cheat ecosystem, while consoles typically ban unauthorized software and mobile platforms rely on curated application stores to reduce exposure (15). Infected devices can also be recruited into botnets to be used for more sophisticated cybercriminal activities, such as Distributed Denial-of-Service (DDoS) attacks, in addition to individual users, showing how a single malware infection can have implications for the security and integrity of the wider gaming ecosystem. Malware infections can also cause financial losses via fraudulent transactions, costly system recovery and the permanent loss of valuable gaming accounts or digital assets. These threats are especially tricky to spot as users looking for cheats usually don't listen to security warnings, turn off protective software or grant elevated system permissions to ensure unofficial programs work as they should. The distribution of third-party content and increasingly sophisticated malware techniques are evolving

as game modification communities. Striking a balance between the benefits of customisation and effective cybersecurity protection will be a long-term challenge for the online gaming industry. Effective cybersecurity ultimately requires a combination of technical safeguards and informed, responsible and security-conscious user behaviour.

(5) Privacy and Behavioural Exploitation

Privacy and behavioural exploitation is the collection, analysis and use of personal and gameplay data to infer attributes outside the gaming environment. Online games today continuously collect behavioral telemetry such as login frequency, play time, purchase history, communication logs, movement patterns, social interactions, and gameplay decisions. Much of this information is collected to improve gameplay experiences and to customize content for individual users. However, studies have shown that aggregated gameplay data can also be analysed to infer sensitive personal characteristics such as personality, gender, emotions, interests, consumption habits and behavioural preferences (17). Individual points of behavioral data may seem insignificant, but their continuous collection and analysis can lead to comprehensive digital profiles of players, often without their full awareness or explicit understanding of the profiling scope. This threat is especially challenging for users to detect as it does not require them to intentionally engage with online gaming services, yet players routinely do so as part of normal gameplay, and so valuable behavioural information can be unknowingly disclosed through everyday in-game activities.

The implications of such data collection go far beyond the traditional privacy concerns. Unlike malware or phishing attacks which typically aim for immediate financial gain or unauthorised system access, behavioural exploitation is focused on the long-term collection of intelligence derived from legitimate user activity. In-game conversations, social interactions and repeated behavioural patterns may inadvertently disclose political opinions, private beliefs or other sensitive personal characteristics. For instance, a player's political preferences could be hypothetically predicted by virtue of their consistent participation in politically themed gaming communities, their regular engagement with political discussions, or the frequency with which they consume political content, when compared to more general behavioural datasets. Live-service, multiplayer and free-to-play games are especially susceptible to this as they constantly track player engagement to optimise matchmaking, monetisation strategies and personalised recommendations. These data-driven systems, while improving the user experience, also increase the amount of behavioural information available for profiling. This data collection is generally done as part of legitimate platform functionality, which is why existing privacy protections are often insufficient and extensive behavioral profiling is possible even if traditional cybersecurity mechanisms have not been compromised. In addition to the privacy risks, the detailed behavioural profiles can be exploited for highly targeted advertising, personalized manipulation or future social engineering attacks, with indirect financial and security consequences for the users. With the increased adoption of AI in online gaming, along with

cross-platform integration and more advanced personalisation systems, the collection, analysis and safeguarding of behavioural data in a transparent and ethical manner will be one of the greatest long-term cybersecurity and privacy challenges facing the gaming industry. Hence, behavioural exploitation is a subtle but very serious cybersecurity threat, showing that sensitive personal information can be inferred from normal gameplay behaviour even in the absence of any traditional security breach.

Table 2 - Comparative Analysis of Major Cybersecurity Issues in Online Gaming

Security Issue	Primary Consequences (Relative Risk)	Key Characteristic
Game Server Exploits	Service disruption, compromised server integrity, unfair gameplay and financial losses (**High**)	Directly targets gaming infrastructure by exploiting vulnerabilities in servers and backend systems.
Distributed Denial-of-Service (DDoS) Attacks	Server outages, increased latency, disrupted gameplay and revenue loss (**High**)	Exhausts network and server resources, preventing legitimate players from accessing gaming services.
Phishing and Social Engineering Attacks	Account compromise, identity theft, financial fraud and virtual asset theft (**High**)	Exploits human behaviour and trust rather than technical vulnerabilities.
Malware and Cheat-Driven Infections	Credential theft, spyware, remote system compromise and persistent malware infections (**Moderate–High**)	Uses unofficial software and cheats to compromise players' devices and gaming accounts.
Privacy and Behavioural Exploitation	Behavioural profiling, privacy violations and unauthorised use of personal data (**Moderate**)	Collects and analyses legitimate gameplay data to infer sensitive behavioural and personal information.

Sources - ***Authors' synthesis based on the reviewed literature (8,10,11,12,13,14,15, and 17)***

The main security challenges identified in the surveyed literature have different attack mechanisms, consequences and overall severity. **Table 2** offers a comparison of these threats, highlighting their relative risk levels and distinguishing characteristics in the online gaming ecosystem.

Table 3.
Comparative Cybersecurity Risk Across Different Gaming Platforms

Gaming Platform	Most Significant Cybersecurity Risks	Relative Cybersecurity Risk	Justification
PC Gaming	Malware and cheat-driven infections, phishing and account compromise	High	Open operating systems, third-party software and unofficial game modifications create a larger attack surface, increasing exposure to malware and credential theft (14, 17, 20).
Mobile Gaming	Phishing, malicious applications, privacy and behavioural exploitation	Moderate–High	Mobile applications require extensive permissions and frequently integrate cloud services, increasing risks related to authentication, data privacy and unauthorised access (18, 20).
Console Gaming	Account compromise, phishing and DDoS attacks	Moderate	Closed operating systems and controlled software distribution significantly reduce malware exposure, although online services and gaming accounts remain attractive targets (10, 19).
Cloud Gaming	Game server exploits, DDoS attacks and data breaches	High	Dependence on centralised cloud infrastructure and continuous internet connectivity increases exposure to infrastructure-level attacks and service disruption (10, 12, 20).
MMORPGs and Live-Service Games	Game server exploits, DDoS attacks, phishing, malware, privacy exploitation and virtual asset theft.	Very High	Persistent online environments, valuable virtual assets, real-time interaction and large player communities create multiple attack opportunities and increase cybersecurity complexity (11–18, 16, 20).
Offline Single-Player Games	Limited malware from unofficial downloads	Low	Minimal online connectivity and limited account-based interactions substantially reduce exposure to network-based cyber threats (10, 13).

Sources – ***Authors' synthesis based on the reviewed literature (8,10,11,12,13,14,15,16,17,18,19,20)***

POSSIBLE SOLUTIONS:

(1) Technical Measures

Technical measures play a key role in online gaming cybersecurity, providing technology-based protections for the gaming infrastructure, user accounts and sensitive data. The key steps include: Multi-factor authentication (MFA) Security authentication protocols Vulnerability disclosure and patching, and AI-driven threat detection. MFA increases the security of your account by requiring two or more ways to verify your identity, making it harder for someone to access your account if they are unauthorised. Regular software patching and disclosure of vulnerabilities enable developers to find and fix security vulnerabilities before they can be exploited. The AI-driven monitoring continuously monitors network traffic and player behaviour for malicious activities such as Distributed Denial-of-Service (DDoS) attacks in real time (8,21-24).

Some of the main cybersecurity issues highlighted in this review can be addressed with technical measures effectively. MFA prevents successful phishing and social engineering attacks by blocking direct account access with compromised credentials. Timely patching reduces the number of exploits in game servers and infections that are caused by malware or cheats (21–23) because patching mitigates known software vulnerabilities before they are exploited by an attacker. AI-based detection improves DDoS attack resilience by identifying abnormal traffic patterns and facilitating quick incident response (23). Together, these measures not only tackle the causes of security-performance trade-offs by embedding security into gaming systems primarily, but also reduce the risks related to the economic value of digital assets by delivering stronger protection to user accounts and virtual assets. But their impact on weak regulatory regimes and on black markets for gaming is limited and needs wider policy and industry-level interventions.

From the practical point of view, the technical approach is the most realistic as the developers have direct control over its implementation and can achieve the improvements in platform security immediately. Although MFA and software updates may cause minor usability costs such as inconvenience during login or brief maintenance periods, the cybersecurity and service reliability benefits are generally far greater, making the technical measures very suitable for modern online gaming platforms (8,21–24).

(2) Spread More Awareness

Cybersecurity awareness and education strengthen the human element of cybersecurity by building the capacity of players to identify, avoid and respond to cyber threats. Much of the attack surface in online gaming does not stem from technical vulnerabilities but from user behaviour. Thus, training the players is a crucial addition to the technological security measures. This includes gamified cybersecurity training, phishing simulations, interactive security quizzes and scenario-based learning embedded in gaming platforms. These methods are especially suitable for

younger gamers who are not aware of cybersecurity, as they increase user engagement and improve secure online practices (25,26).

Mostly, cybersecurity awareness is a defence against phishing and social engineering attacks, training players to spot fake emails, fake login pages and suspicious in-game messages before they give away sensitive information. It also reduces malware and cheat-based infections by discouraging players from downloading unofficial mods, cheats or third-party software from untrusted sources. Awareness programmes address the digital illiteracy identified as a key underlying cause of cybersecurity issues in online gaming by transforming users from vulnerable targets into informed participants who can make safer security decisions. However, awareness programmes have limited impact on game server exploits, distributed denial-of-service (DDoS) attacks, weak regulatory frameworks and gaming black markets, as these threats are predominantly based on technical vulnerabilities, infrastructure-level attacks or broader economic and legal factors.

However, unlike technical security controls, cybersecurity awareness programs have little to no impact on gameplay performance. Educational content is most often delivered through onboarding tutorials, optional learning modules or periodic security campaigns, rather than during live gameplay. But poorly designed or overused awareness prompts can lead to reduced user engagement or be ignored over time. This suggests that cybersecurity awareness is most effective when it is an ongoing and interactive process that occurs in conjunction with technical safeguards, as both human behaviour and technological defences can contribute to a more secure online gaming environment (25,26).

(3) Industry Collaboration

As the online gaming infrastructure becomes more and more interconnected, cybersecurity efforts can no longer be left to individual developers or publishers. Today's gaming ecosystem includes several players, such as game developers, publishers, cloud service providers, cybersecurity companies, payment processors, and regulatory bodies that help keep platforms secure. Industry collaboration is the cooperative sharing of cyber threat intelligence, vulnerability information, attack indicators and security best practices between these stakeholders to increase collective resilience to emerging cyber threats. Cyber Threat Intelligence (CTI) sharing enables organisations to quickly share information on new vulnerabilities, malware signatures, phishing campaigns and attack patterns so that security teams can act proactively before threats are propagated across multiple gaming platforms (27).

Industry collaboration is a way to solve many of the major problems facing cybersecurity, such as phishing attacks, malware infections, Distributed Denial-of-Service (DDoS) attacks, server exploits and account compromise. Sharing indicators of compromise, vulnerability disclosures, and real-time threat intelligence allows organisations to quickly apply security patches, upgrade

intrusion detection systems and block malicious infrastructure before attackers exploit similar weaknesses across multiple platforms. This collaborative approach also tackles underlying issues such as the absence of harmonised cybersecurity standards by promoting consistent security practices, coordinated vulnerability disclosure and shared defensive strategies across the gaming industry. Working together to monitor suspicious trading patterns and compromised accounts can also limit the flow of stolen digital assets and disrupt gaming black markets. However, collaboration between industries has little effect on digital illiteracy or the financial motivation behind cybercrime. This is because these two issues stem from user behaviour and the economic value of virtual assets, not the lack of coordination between organisations.

Industry collaboration is very practical from an implementation perspective for large game developers and publishers who already have dedicated cybersecurity teams, Security Operations Centres (SOCs) and incident response capabilities. However, smaller developers may face financial, technical and organisational barriers to participation in formal threat-sharing initiatives due to limited cybersecurity expertise and infrastructure. As collaborative activities mainly occur between organisations and not on players' devices, this solution has virtually no direct impact on gameplay performance, latency or user experience. Rather, the benefits are felt indirectly in the form of faster vulnerability remediation, improved platform stability and less exposure to large-scale cyberattacks. Industry collaboration, therefore, provides an effective defence mechanism at the ecosystem level, strengthening collective cyber resilience across the online gaming industry and complementing technical security controls and user awareness initiatives.

(4) Legal and Regulatory measures

The transnational nature of online gaming requires legal and regulatory measures beyond the technical safeguards adopted by individual organisations. Laws and regulations include the making and enforcement of laws, international agreements and regulatory frameworks that govern data protection, cybercrime, the protection of digital assets and the security of online platforms. Legislation like the General Data Protection Regulation (GDPR) sets legal requirements for organisations to protect users' personal data. Cooperation at the international level allows governments and law enforcement agencies to investigate and prosecute cybercriminals operating in different jurisdictions (6,28).

Strong legal and regulatory frameworks can help confront a variety of cybersecurity issues, such as data breaches, account theft, identity fraud, phishing campaigns, and illegal trading of stolen digital assets. Regulatory frameworks provide compulsory cybersecurity requirements, data protection duties and legal consequences for cybercrime, which encourage organisations to implement better security controls and increase compliance with recognised cybersecurity standards. International cooperation enhances cyber security through cross-border investigations, sharing of intelligence and coordinated law enforcement actions against organised cybercriminal groups exploiting differences in national legislation. Consequently, legal regulation directly

addresses the absence of harmonised cybersecurity standards and limits the proliferation of gaming black markets via enhanced legal enforcement. But the impact of legal measures on digital illiteracy is limited, and they are unable to eliminate the financial motives of cybercriminals. Therefore, complementary technical and educational solutions are no less important.

Legal and regulatory measures are very practical for implementation at the governmental and industry level because compliance requirements can be embedded in organisational security policies and software development practices. But differences in national laws, jurisdictional limitations and uneven enforcement can undermine their effectiveness against cybercriminals operating across international borders. These measures are largely driven by law enforcement, organisational governance and legislation, rather than gameplay itself, and thus have little to no direct impact on game performance, latency or user experience. Instead, players indirectly benefit from better protection of personal data, accountability of gaming companies and legal deterrence against cybercrime. Thus, strong legal and regulatory frameworks are a key foundation for long-term cyber resilience, as they complement technical security measures, cyber awareness programmes and industry collaboration initiatives.

(5) Emerging Research Directions

The rapidly changing world of online gaming continues to present cybersecurity challenges that existing technical, educational or regulatory measures cannot always fully resolve. As a result, the investigation of emerging technologies as potential long-term solutions to enhance the security, privacy and resilience of future gaming ecosystems is increasing in popularity. Current studies are mostly on blockchain technology for secure digital asset management, privacy-preserving analytics for responsible data processing and identity management mechanisms for virtual and metaverse environments (29,30).

Blockchain technology's decentralised and immutable architecture has garnered considerable interest due to its ability to provide transparent records of digital asset ownership and in-game transactions without the need for a single trusted authority. This reduces the risk of fraudulent asset transfers, account manipulation and unauthorised modification of ownership records, mitigating the cybersecurity issues associated with virtual asset theft and gaming black markets. Likewise, privacy-preserving analytics, such as differential privacy and federated learning techniques, allow developers to analyse player behaviour for security monitoring, anomaly detection, and cheat identification while limiting the exposure of personally identifiable information. These technologies also help meet data protection regulations by minimizing collection and disclosure of sensitive user data that is not needed. Moreover, as online gaming is reaching virtual reality and metaverse platforms, new research is constantly emerging on secure avatar authentication, decentralised digital identity management and cross-platform identity protection in order to avoid impersonation and identity fraud.

Despite the promising potential, these technologies are still at an early stage of practical implementation in the gaming industry. Blockchain-based systems are often plagued by transaction scalability, storage overhead, interoperability with existing gaming infrastructures and computational overhead of distributed consensus mechanisms. Incorporating these elements directly into gameplay, it could lead to transaction lag, operational costs for the developers, and lower responsiveness that is expected in fast-paced online games. Similarly, privacy-preserving analytics such as differential privacy and federated learning require additional computational resources and may reduce the accuracy of behavioural analysis, as intentional data modifications may reduce the accuracy of cheat detection and real-time security monitoring. From an implementation perspective, these technologies are more feasible at present for large gaming companies with deep pockets, advanced cloud infrastructure and dedicated cybersecurity teams, while smaller developers may face some significant economic and technical barriers to deployment. In addition, metaverse-based gaming environments present further research challenges in terms of avatar identity verification, secure cross-platform authentication and protection of digital identities across interconnected virtual worlds. Therefore, while these technologies are unlikely to substitute traditional cybersecurity measures in the short term, they constitute promising long-term research avenues that can substantially enhance the security, privacy and resilience of online gaming ecosystems as technological capabilities continue to develop.

Table 4 - Comparative analysis of cybersecurity solutions in online gaming					
Solution	**Causes Mitigated**	**Issues Mitigated**	**Effectiveness**	**Impact on Performance**	**Practicality (User / Company)**
Technical Security Measures	Digital illiteracy (partial), Security–performance trade-offs	Server exploits, DDoS attacks, Phishing & social engineering, Malware & cheat-driven infections, Privacy & behavioural exploitation	Very High	Slight latency	Moderate / High
Cybersecurity Awareness	Digital illiteracy	Phishing & social engineering, Malware & cheat-driven infections	High	Negligible	High / High
Industry Collaboration	Weak regulations, Gaming black markets	Server exploits, DDoS attacks, Phishing & social engineering, Malware & cheat-driven infections	High	Minimal	Low / Moderate–High
Legal & Regulatory Measures	Weak regulations, Gaming black markets	Privacy & behavioural exploitation, Phishing & social engineering	Moderate–High	None	Moderate / High
Emerging Research	Economic value of digital assets	Privacy & behavioural exploitation, Malware & cheat-driven infections	Moderate–High	Moderate overhead	Low–Moderate / Moderate
Sources - ***Authors' synthesis based on the reviewed literature (6 and 21–30)***					

Table 4 compares the efficiency and applicability of the cybersecurity solutions discussed. There is no one-size-fits-all solution since each solution addresses different root causes and cybersecurity issues. Therefore, enhancing cybersecurity in online gaming requires a layered approach that integrates complementary technical, educational, collaborative, regulatory and emerging technological measures.

CONCLUSION

The literature reviewed shows that cybersecurity in online gaming is a multi-dimensional problem arising from the interaction between human behaviour, economic incentives, technological limitations and regulatory gaps. The identified causes, including digital illiteracy, the increasing value of digital assets, inconsistent legal frameworks, trade-offs between security and performance, and black markets for gaming, contribute to cybersecurity issues such as server exploits, Distributed Denial-of-Service (DDoS) attacks, phishing, malware, privacy breaches, and account compromise. The review also notes that these interlinked challenges cannot be addressed by a single cybersecurity solution. Technical security measures, cybersecurity awareness, industry collaboration, legal and regulatory frameworks and emerging technologies all address different causes and security issues, but also have their own challenges in implementation, practical limitations and performance trade-offs. Therefore, effective online gaming cybersecurity is a layered, collaborative effort, where these strategies work together and not in isolation. As online gaming becomes more a part of the digital economy, cloud gaming, and metaverse environments, future research should look at the development of scalable, practical, and user-centric security solutions that balance cybersecurity, privacy, and gameplay performance. Enhanced collaboration between developers, industry stakeholders, researchers, policymakers and players will be crucial to building a secure and sustainable online gaming ecosystem.

LIMITATIONS OF THE STUDY

Although this review offers a thorough synthesis of the existing literature on cybersecurity issues in online gaming, there are some limitations to its scope. This study is based solely on secondary literature and does not incorporate any primary empirical data or experimental validation. Includes a legislation reference(6) from 2016, as the law has not changed since then. Moreover, the review involves a broad analytical point of view, which highlights the identification, evaluation and comparison of the cybersecurity causes, issues and mitigation strategies rather than the deep technical analysis of some security algorithms, cryptographic protocols or network architectures. The comparative evaluations presented in the tables are qualitative syntheses based on the reviewed literature and should thus be interpreted as evidence-based assessments rather than quantitative measurements. Due to the rapid development of cybersecurity and online gaming technologies, newly emerging threats and defensive approaches may not be fully covered within the scope of this review.

REFERENCES

1. Ng, Chiu Yeong, and Mohammad Khatim Bin Hasan. "Cybersecurity serious games development: A systematic review." *Computers & Security* 150 (2025): 104307.
2. Khadka, Kalam, and Abu Barkat Ullah. "Human factors in cybersecurity: an interdisciplinary review and framework proposal: K. Khadka, AB Ullah." *International Journal of Information Security* 24.3 (2025): 119.
3. Houser, Adam M., and Matthew L. Bolton. "Formal mental models for human-centred cybersecurity." *International Journal of Human–Computer Interaction* 41.2 (2025): 1414-1430.
4. Gibson, Erin, et al. "The relationship between videogame micro-transactions and problem gaming and gambling: A systematic review." *Computers in Human Behaviour* 131 (2022): 107219.
5. Higgs, James, and Stephen Flowerday. "Cybercrime and virtual laundering in video game marketplaces: A Bayesian P-inductive argument." *Technology in Society* 83 (2025): 102978.
6. Regulation, Protection. "Regulation (EU) 2016/679 of the European Parliament and of the Council." *Regulation (EU)* 679.2016 (2016): 10-3.
7. Prasad, Nilantha, et al. "A survey of cyber threat attribution: Challenges, techniques, and future directions." *Computers & Security* (2025): 104606.
8. Bryant, Blake, and Hossein Saiedian. "An evaluation of videogame network architecture performance and security." *Computer networks* 192 (2021): 108128.
9. Lee, Eunjo, et al. "No silk road for online gamers! using social network analysis to unveil black markets in online games." *Proceedings of the 2018 World Wide Web Conference*. 2018.
10. Gavrić, Nikola, and Živko Bojović. "Security Concerns in MMO Games—Analysis of a Potent Application Layer DDoS Threat." *Sensors* 22.20 (2022): 7791.

11. Klostermeyer, Philip, et al. "Skipping the security side quests: A qualitative study on security practices and challenges in game development." *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security*. 2024.

12. Bhardwaj, Aanshi, et al. "Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions." *Computer Science Review* 39 (2021): 100332.

13. Abdillah, Rahmad, et al. "Phishing classification techniques: A systematic literature review." *IEEE Access* 10 (2022): 41574-41591.

14. Syafitri, Wenni, et al. *"Social Engineering Attacks Prevention: A Systematic Literature Review." IEEE Access*, vol. 10, 2022. https://doi.org/10.1109/ACCESS.2022.3162594.

15. Han, Mee Lan, Byung Il Kwak, and Huy Kang Kim. "Cheating and detection method in massively multiplayer online role-playing game: systematic literature review." *IEEe Access* 10 (2022): 49050-49063.

16. Iqbal, Asif, et al. "Unveiling the connection between malware and pirated software in Southeast Asian countries: A case study." *IEEE Open Journal of the Computer Society* 5 (2024): 62-72.

17. Kröger, Jacob Leon, et al. "Surveilling the gamers: Privacy impacts of the video game industry." *Kröger J., Raschke P., Percy Campbell J. and Ullrich S., Surveilling the Gamers: Privacy Impacts of the Video Game Industry, Entertainment Computing* 44 (2023): 100537.

18. Jeon, Sanghoon, and Huy Kang Kim. "TZMon: Improving mobile game security with ARM trustzone." *Computers & Security* 109 (2021): 102391.

19. Di Domenico, Andrea, et al. "A network analysis on cloud gaming: Stadia, GeForce Now and psnow." *Network* 1.3 (2021): 247-260.

20. Joens, Alexander, Ananth A. Jillepalli, and Frederick T. Sheldon. "Trustworthy High-Performance Multiplayer Games with Trust-but-Verify Protocol Sensor Validation." *Sensors* 24.14 (2024): 4737.

21. Ang, Kok Wee, Eyasu Getahun Chekole, and Jianying Zhou. "Unveiling the covert vulnerabilities in multi-factor authentication protocols: a systematic review and security analysis." *ACM Computing Surveys* 57.11 (2025): 1-37.

22. Liu, Shuhan, et al. "An empirical study on vulnerability disclosure management of open source software systems." *ACM Transactions on Software Engineering and Methodology* 34.7 (2025): 1-31.

23. Woo, Seunghoon, Eunjin Choi, and Heejo Lee. "A large-scale analysis of the effectiveness of publicly reported security patches." *Computers & Security* 148 (2025): 104181.

24. Najafimehr, Mohammad, Sajjad Zarifzadeh, and Seyedakbar Mostafavi. "DDoS attacks and machine‐learning‐based detection methods: A survey and taxonomy." *Engineering Reports* 5.12 (2023): e12697.

25. Weeratunge, Nipuna Hiranya, Rune Hjelsvold, and Basel Katt. "A systematic scoping review on game-based cybersecurity awareness education: NH Weeratunge et al." *International Journal of Information Security* 25.2 (2026): 71.

26. Yeoh, William, et al. "Simulated phishing attack and embedded training campaign." *Journal of Computer Information Systems* 62.4 (2022): 802-821.

27. Wagner, Thomas D., et al. "Cyber threat intelligence sharing: Survey and research directions." *Computers & Security* 87 (2019): 101589.

28. Wang, Xin. "Global (re-) framing of cybercrime: An emerging common interest in flux of competing normative powers?" *Leiden Journal of International Law* 38.2 (2025): 235-261.

29. Rishiwal, Vinay, et al. "Blockchain-secure gaming environments: A comprehensive survey." *IEEE Access* 12 (2024): 183466-183488.

30. Hassan, Muneeb Ul, Mubashir Husain Rehmani, and Jinjun Chen. "Differential privacy in blockchain technology: A futuristic approach." *Journal of Parallel and Distributed Computing* 145 (2020): 50-74.