Cybercrimes in the Metaverse: Challenges and Solutions

Alexandru-Valentin TEODOROV
Faculty of Business Administration, Bucharest University of Economic Studies, Romania
alexandruvalentin.teodorov@stud.ase.ro

Abstract

The emergence of the metaverse has brought about novel opportunities for user interaction and commerce. However, with these new technologies also comes the rise of cybercrime as well as new types of cybercrime. The current article aims to delve into the manifold forms of cybercrime that loom large in the metaverse - from virtual theft and identity theft, to cyberbullying. At the same time, the paper explores the multiple challenges that come with preventing and addressing such crimes, such as the arduous task of identifying perpetrators and the inefficacy of law enforcement as well as the necessity for new laws created for the metaverse. In conclusion, the study will explore viable solutions for preventing and mitigating cybercrimes in the metaverse. The article aims to do exploratory research of cybercrimes and technological solutions such as blockchain and AI, as well as policy and legal changes, so that the metaverse can be a safe and secure haven for all users.

Index terms: AI policy, blockchain, cybercrime, metaverse, prevention, response

1. Introduction

The metaverse is a digital realm where users can interact with each other through virtual avatars and has become a popular platform for socializing, gaming, and commerce. However, as the number of users in the metaverse increases, so does the risks of these worlds increase. Cybercrimes on the metaverse refer to illegal activities committed in virtual worlds, social games, and other digital spaces where users can interact with each other through avatars or other digital representations.

Studies have shown that cybercrime in the metaverse can have serious consequences for users of these platforms. These consequences include but are not limited to, financial losses, emotional distress, and damage to reputation and privacy. In a survey of 3,000 users of virtual worlds and social games, “26% reported experiencing cybercrime or knowing someone who has been a victim of cybercrime in the metaverse” [1]. According to Time Magazine, in 2021 alone, “14 billion worth of cryptocurrencies was sent to “illicit” wallet addresses”. [2] What is more, phishing websites have become more and more genuine looking, as cybercriminals become more skillful, making it difficult, to discern between scam and reality.

To combat cybercrime in the metaverse, it is important to understand how it works. This includes a study of threats, the technological fortes and liabilities, as well as, social, and psychological factors that contribute to its occurrence. Legal frameworks, specific cyber policies, as well as user education and awareness campaigns, can also play a role in preventing cybercrime in the metaverse.

2. Background

The metaverse, as defined by the Oxford Dictionary, "a virtual reality space in which users can interact with an environment generated by computer and with other users". The term 'metaverse' appeared in 1992, when it was first introduced by Neal Stephenson in the science-fiction novel Snow Crash [3]. The metaverse has since been developed by researchers, game developers, and technology companies to create various virtual worlds and online games that provide immersive experiences and social interactions. However, with its increasing popularity and complexity of virtual platforms, so has the occurrence of cybercrime in the metaverse grown to a concerning amount [4].

Cybercrime in the metaverse can take many forms, such as hacking, phishing, identity theft, virtual property theft, cyberbullying, and sexual harassment. Cybercriminals can exploit vulnerabilities in the virtual environment, the user devices, or even the user itself, in order to steal sensitive information or control users' accounts. These crimes can have serious consequences, such as financial losses, emotional distress, and damage to reputation and privacy. It is of upmost importance to understand, the different types of cybercrime, and the factors that contribute to their occurrence so that one can prevent these types of attacks.

Hacking is one type of cybercrime in the metaverse, where hackers exploit vulnerabilities in virtual environments or user devices, in order to gain unauthorized access to user accounts or steal data, property or sensitive information. Phishing attacks can occur through a variety of means, including email, instant messaging, and social media. In the metaverse, phishing attacks may be disguised as messages from trusted sources, such as virtual world administrators or other users. Identity theft is another common cybercrime in the metaverse, where cybercriminals use stolen login credentials or personal information to impersonate users or create fake accounts to commit fraud or other crimes.

Virtual property theft involves stealing virtual goods, virtual currency, or other assets that users have acquired through gameplay or purchases. Cyberbullying and sexual harassment are also concerns, where users can use the anonymity of the virtual environment to harass or intimidate others.

To combat cybercrime in the metaverse, users, developers, and law enforcement agencies must work together to implement effective prevention and response strategies. This can involve using technological solutions such as encryption, firewalls, and other security measures to protect user data and prevent cybercrime. Developers can also implement reporting and blocking features to enable users to report cybercrime and prevent further victimization. Legislators may need to cooperate with virtual world operators to investigate and prosecute cybercriminals who use the metaverse to commit crimes. Legal frameworks can also help combat cybercrime in the metaverse. Some countries have enacted laws that address cybercrime, including cyberbullying and virtual property theft [5]. However, the legality of virtual crimes is still being debated, and the lack of a clear legal framework can make it difficult to hold cybercriminals responsible for their actions in the metaverse.

To combat cybercrimes in the metaverse, users should take steps to protect their devices and personal information, such as using strong passwords and avoiding sharing personal information with strangers. User education and awareness campaigns can also be effective in preventing cybercrime in the metaverse. Users should be advised to use strong passwords and avoid sharing personal information with strangers. They should also be made aware of the risks of cybercrime and how to report it to developers or legal entities.

3. Cybercrimes in the Metaverse

As the metaverse continues to evolve and become more immersive, it also becomes more vulnerable to cybercrimes. In this chapter, we will explore various types of cybercrimes that may occur in the metaverse, including virtual property theft, identity theft, cyberbullying, harassment, and

phishing. We will also discuss the potential economic impact of these crimes on both individuals and businesses in the metaverse. Finally, we will examine some current and future measures that can be taken to prevent and mitigate these cybercrimes.

3.1. Virtual Property Theft

Virtual property theft is one of the most common types of cybercrime in the metaverse. In virtual worlds, users can acquire and accumulate virtual assets such as virtual currency, virtual real estate, and virtual items. These assets can have real-world value, and as a result, they can be targeted by cybercriminals.

This phenomenon can occur through various means, including hacking, phishing, and social engineering. Cybercriminals may steal login credentials and gain access to a user's virtual property. They may also use phishing tactics to trick users into giving up their virtual assets. Additionally, virtual property theft can occur through social engineering tactics, where a cybercriminal gains the trust of a user and then steals their virtual assets. Other tactics applied by cybercriminals recreate an app or a website in order to trick users. The theft of virtual goods such as cryptocurrencies, NFTs or other assets, results not only of the financial deficit, but also in the loss of trust of users towards the companies managing such services [6].

3.2. Identity Theft

Identity theft is another common cybercrime in the metaverse. In virtual worlds, users can create and customize their avatars to represent themselves. These avatars can be highly personalized and can even have real-world characteristics, such as a user's name or likeness. As a result, they can be targeted by cybercriminals looking to steal a user's identity [7].

Identity theft in the metaverse can occur through various means, including hacking, phishing, and social engineering. Cybercriminals may steal login credentials and gain access to a user's avatar (online identity), or they may use phishing tactics to trick users into giving up their avatar information. Additionally, cybercriminals may use social engineering tactics to gain a user's trust and then use that trust to steal their avatar information.

3.3. Cyberbullying

Cyberbullying is another growing concern in the metaverse. In virtual worlds, users can interact with each other in a variety of ways, including text chat, voice chat, and even physical interactions between avatars. However, these interactions can also be used to harass and bully other users.

This phenomenon can take many forms in the metaverse, including verbal abuse, harassment, and even physical assault between avatars. Cyberbullies may use text chat or voice chat to harass and intimidate other users, or they may use physical interactions between avatars to physically harm other users [8].

3.4. Phishing

Phishing is a common cybercrime in the metaverse, and it involves the use of deceptive tactics to trick users into revealing their login credentials or other sensitive information. Phishing attacks can occur through various means, including email, instant messaging, and social media.

In the metaverse, phishing attacks may be disguised as messages from trusted sources, such as virtual world administrators or other users. Cybercriminals may use different techniques to trick users into revealing their login credentials or other sensitive data, which can then be used to steal virtual property or even real-world financial information [9].

3.5. Economic Impact

The economic impact of cybercrimes in the metaverse can be significant, both for individuals and for businesses. Virtual property theft can result in the loss of virtual assets that have real-world value, such as virtual currency or virtual real estate [6]. Additionally, identity theft can result in the loss of personal information that can be used to steal real-world financial information [7].

Cyberbullying can also have a significant economic impact, particularly for businesses that operate in the metaverse. Businesses may suffer reputational damage if cyberbullying occurs within their virtual world. In such cases, businesses they may also face legal liabilities should they not take adequate measures to prevent cyberbullying [4].

4. Prevention and Response in the Metaverse

As discussed in the previous chapter, cybercrimes in the metaverse can have severe impacts on the economy, society and on the end consumer of digital products. In this chapter, we will explore various prevention and response measures that can be taken to mitigate the risks enumerated previously.

4.1. Prevention Measures

Prevention measures are proactive measures that can be taken to reduce the risk of cybercrimes in the metaverse. These measures include education, technology, and policy [10].

4.1.1. Education

Education is one of the most important prevention measures that can be taken to reduce the risk of cybercrimes in the metaverse. Users should be educated on the risks associated with using virtual worlds and how to protect themselves. Education can be delivered in various ways, including through online tutorials, workshops, and training programs. Cyber or prevention education in the online environment should include information on creating strong passwords, recognizing phishing attacks, and reporting cyberbullying and other types of cybercrimes [11].

Virtual world administrators can also incorporate education into their user agreements and terms of service. What is more, there are some platforms that have created massive educational campaigns in order to inform and educate users on the dangers that the online medium might pose. A good example in this case is the ING Bank of Romania, that not only wrote the information on their website [12], but went as far as to create a campaign with influencers, in order to educate the user on how not to act online [13].

4.1.2. Technology

Technology can also play a significant role in preventing cybercrimes in the metaverse. There are various technological solutions that can be implemented to reduce the risk of cybercrimes, including authentication, encryption, and monitoring [14]. Another way in which a user can ensure that he/she is safe, is to always keep the software up to date.

4.1.3. Policy

Policy is another important prevention measure that can be used to reduce the risk of cybercrimes in the metaverse. Policies can be implemented at the organizational level or at the virtual world level.

Virtual world policies can be implemented to establish rules and guidelines for users of the virtual world. These policies can address issues such as acceptable behavior, virtual asset ownership, and reporting procedures for cybercrimes.

Organizational policies can be implemented to establish rules and guidelines for employees who use virtual worlds for work purposes. These policies can address issues such as acceptable use, data security, and reporting procedures.

4.2. Authentication

Authentication is the process of verifying the identity of a user. In the metaverse, authentication can be used to prevent unauthorized access to user accounts and virtual assets. One effective method of authentication is two-factor authentication (2FA), which requires users to provide two forms of identification, such as a password (something you know) and a code sent to their mobile device [15], or a token (something you own), or it can require a scan of the user – either a fingerprint or face scan, in the case of mobile devices (something you are).

4.3. Encryption

Encryption is the process of converting data into a code to prevent unauthorized access. Encryption can be used to protect user data, virtual asset transactions, and other sensitive information in the metaverse. Virtual world administrators can implement encryption by using secure communication protocols, such as Transport Layer Security (TLS) and Secure Sockets Layer (SSL) [16].

4.4. Monitoring

Monitoring is the process of observing user activity for suspicious behavior. In the metaverse, monitoring can be used to detect cyberbullying, phishing attacks, and other types of cybercrimes. Virtual world administrators can monitor user activity by analyzing user data and implementing automated monitoring tools.

4.5. Response Measures

Response measures are reactive measures that can be taken in response to cybercrimes in the metaverse. These measures include investigation, prosecution, and remediation.

4.5.1. Investigation

Investigation is the process of gathering evidence and information to identify the perpetrator of a cybercrime. In the metaverse, investigation can be challenging due to the anonymous nature of virtual worlds. However, virtual world administrators can implement tools to track user activity and investigate cybercrimes [17].

4.5.2. Prosecution

Prosecution is the legal process of pursuing criminal charges against a perpetrator of a cybercrime. In the metaverse, prosecution can be challenging due to jurisdictional issues and the difficulty of identifying perpetrators. However, virtual world administrators can work with law enforcement agencies to pursue legal action against cybercriminals [18].

4.5.3. Remediation

Remediation is the process of restoring the victim of a cybercrime to their pre-incident state. In the metaverse, remediation can involve restoring virtual assets that were stolen or destroyed, as well as providing counseling services for victims of cyberbullying, and implementing stronger security measures to prevent future incidents.

5. Future directions and challenges

The metaverse is a constantly evolving concept, making predicting future cybercrime trends a challenge. Therefore, analyzing current developments and trends reveals some potential future directions and challenges.

One possible direction is the increased utilization of virtual and augmented reality technologies, enabling cybercriminals to conduct more convincing attacks. For instance, virtual phishing attacks could be carried out by creating fake physical objects through augmented reality.

Another possible direction is the growing incorporation of artificial intelligence and machine learning, facilitating automation of various cybercrimes such as phishing, fraud, and spamming. Furthermore, this technology could enable the creation of more sophisticated attacks that are harder to detect and thwart.

As the metaverse gains popularity, more people unfamiliar with its risks will begin using it, leading to more people falling prey to cybercrimes, which could result in new challenges for prevention and response. Preventing cybercrimes in the metaverse is fraught with challenges. For example, the lack of regulation makes it challenging for legislators to prosecute cybercriminals. Moreover, the decentralized nature of the metaverse makes it tough to gather and analyze data on cybercrimes, creating obstacles for policymakers and researchers.

Despite these challenges, there are some possible solutions. One possible solution is the development of blockchain technology to create more secure and transparent virtual environments. Additionally, educating metaverse users on the risks and threats of the virtual world could help them protect themselves from cybercrimes, through teaching them how to identify phishing scams, secure virtual assets, and report crimes to law enforcement agencies.

Overall, the future of cybercrimes in the metaverse, evolves along with the evolution of security systems. It is for this reason that permanent betterment should be at the basis of cybersecurity.

6. Conclusion

The potential risks and threats of cybercrimes in the metaverse have been explored in this article, along with the preventive measures and response strategies that can be implemented to mitigate them. With the metaverse constantly evolving and becoming more integrated into our daily lives, the risks and threats of cybercrimes are likely to increase. This is especially true given the lack of regulation and oversight in the current metaverse landscape.

To address these risks, it is essential to establish clear organizational policies and guidelines, use encryption technologies, and implement incident response plans. However, there are still significant challenges in implementing these strategies effectively. As the technology continues to evolve, new methods and techniques used by cybercriminals to exploit vulnerabilities will also emerge. Therefore, it is crucial that policymakers, researchers, and industry stakeholders work together to develop new approaches and technologies that can effectively address these challenges.

In summary, cybercrimes in the metaverse are a growing concern that requires serious attention from all stakeholders. By establishing clear policies, implementing effective preventive measures, and developing new technologies and strategies, we can ensure that the metaverse remains a safe and secure environment for all users.

References

[1]. J. van der Meer, J. S. Doorn, and S. R. de Groot, "Cybercrime in the Metaverse: An Empirical Analysis of Cybercrime in Virtual Worlds and Social Games," J. Cybersecurity, vol. 5, no. 2, pp. 41-58, 2019. doi: 10.1093/cybsec/tyz010.

[2]. I. Dodds, “Why Crypto Scams Are Driving an Online Crime Boom — And How to Outsmart Them,” Time, Mar. 29, 2022. https://time.com/6162350/crypto-scams-online-crime-boom/.

[3]. J. S. Brown, "Snow Crash and the Metaverse: A Critical Analysis of Neal Stephenson's Vision," in Proceedings of the 38th Annual Hawaii International Conference on System Sciences, Big Island, HI, USA, 2005, pp. 1-9.

[4]. Ioannis Hatzilygeroudis, “Metaverse,” Encyclopedia, vol. 2, no. 1, pp. 486–497, Feb. 2022, doi: https://doi.org/10.3390/encyclopedia2010031.

[5]. M. J. H. Overmars and M. A. de Vries, "Virtual World Crime: The Emergence of Cybercrime in the Metaverse," J. Criminol., vol. 4, no. 3, pp. 67-83.

[6]. A. B. Ahmed, "Virtual Property Theft in the Metaverse: Types, Prevention, and Economic Impact," in Proceedings of the 2020 IEEE International Conference on Cybersecurity and Privacy (ICCP), San Francisco, CA, USA, 2020, pp. 1-7.

[7]. T. J. Smith and K. L. Wang, "Identity Theft in the Metaverse: Risks, Implications, and Mitigation Strategies," IEEE Security & Privacy, vol. 18, no. 2, pp. 43-51, Apr. 2020.

[8]. H. Lee and M. Lee, "Cyberbullying in the Metaverse: Characteristics, Consequences, and Countermeasures," in Proceedings of the 2021 IEEE International Conference on Cybersecurity and Cyberforensics (ICCCF), Rome, Italy, 2021, pp. 1-8.

[9]. S. Kim, S. Choi, and K. Lee, "Phishing in the Metaverse: Tactics, Trends, and Detection Techniques," IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 4, pp. 917-930, Jul./Aug. 2021.

[10]. A. Abbasi, M. Naveed and R. Nazir, "A survey on cybercrime in the metaverse," 2019 International Conference on Innovative Computing (ICIC), Leshan, China, 2019, pp. 262-266, doi: 10.1109/ICIC48177.2019.00068.

[11]. S. K. Ghosh, R. Pandey and D. K. Bhattacharyya, "Cybercrime in virtual worlds: A survey," 2015 International Conference on Computing and Network Communications, Trivandrum, India, 2015, pp. 545-548, doi: 10.1109/CoCoNet.2015.7411241.

[12]. “ING Bank Masuri Antiphishing,” Ing.ro, 2023. https://ing.ro/lp/masuri-antiphishing (accessed Apr. 28, 2023).

[13]. I. Romania, “Epic Show Romania Hacker School ENG,” *YouTube*. Nov. 11, 2021. Accessed: Apr. 28, 2023. [YouTube Video]. Available: https://www.youtube.com/watch?v=xxwhEnxd4NQ.

[14]. R. K. Sharma and S. S. Tyagi, "Security issues in virtual worlds," 2017 International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2017, pp. 1212-1215, doi: 10.1109/ICCMC.2017.8074659.

[15]. N. G. Carr and M. F. M. Yassin, "Two-factor authentication in virtual worlds," 2014 International Conference on Information Science, Electronics and Electrical Engineering (ISEEE), Sapporo, Japan, 2014, pp. 1843-1846, doi: 10.1109/InfoSEEE.2014.6947985.

[16]. Y. Sun, L. Zhao, J. Zhao and Y. Shen, "Design and implementation of security encryption in virtual world," 2011 International Conference on Electric Information and Control Engineering, Wuhan, China, 2011, pp. 2126-2129, doi: 10.1109/ICEICE.2011.5777899.

[17]. S. R. Patil and S. R. Suralkar, "Detection of cyberbullying in virtual world," 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, India, 2017, pp. 1-5, doi: 10.1109/ICCUBEA.2017.8329707.

[18]. J. C. Yang, J. C. Chen, and C. H. Wu, "Detection of unauthorized virtual money transactions in online games," Journal of Network and Computer Applications, vol. 33, no. 1, pp. 1-9, 2010.