Who is Threatening My Avatar in Metaverse?

Mădălina ZAMFIR, Andreea - Cătălina CRĂCIUN
National Institute for Research and Development in Informatics - ICI Bucharest
madalina.zamfir@ici.ro, andreea.craciun@ici.ro

Abstract: This paper investigated the potential key aspects related to cybersecurity in Metaverse, regarding cyber threats and cyber crimes, challenges and risks, along with potential security measures that must be taken into account for a safe activity and an enjoyable user experience. Starting from real cases of security incidents in Metaverse, potential strategies and principles for ensuring cybersecurity in virtual environments were presented. An analysis of the user-avatar relation was carried out to synthesize the benefits and risks that the user may face in the virtual environment, when using digital devices and immersive and emergent technologies, in the interaction and collaboration with the other avatars.

Keywords: Metaverse, cybersecurity, cyberbullying, cybercrime, avatar, metalepsis.

INTRODUCTION

Metaverse is a concept that combines physical and virtual reality and can be accessed through the Internet and digital devices, and the powerful technologies on which it is built allow users to have remarkable immersive experiences. Immersive technologies such as extended reality (XR) and Head Mounted Displays (HMDs) make it easier to connect people to the virtual world and virtual content (Chow et al., 2022). As these technologies develop, the popularity of the Metaverse is growing rapidly, and ensuring the security of personal data and minimizing the risks associated with digital interactions and transactions are crucial (Analytics Insight, 2023), (Pew Research Center, 2022).

The success of a Metaverse platform depends on the confidence users have in using it (TechTarget, 2023). Whether it is for leisure, study or business, cybersecurity is important, especially since users are already aware of cyber security regarding data breaches and cyber-attacks that they know about in the real world (TechTarget, 2023), (Ene & Savu, 2023).

Both businesses and consumers consider privacy and cybersecurity issues to be the primary concern in adopting Metaverse (PWC, 2022). According to a study by PWC, (2022) 66% of participating companies said they are actively participating in Metaverse technology, either by building proofs of concepts, testing case studies or generating revenue from transactions, while 55 % of consumers find Metaverse captivating.

https://doi.org/10.54851/v5i2y202308

Only 9% of them said they use existing Metaverse environments. 82% of companies plan to include Metaverse in their business plans in the next 3 years.

This paper aims to address the development in the field of Metaverse security and present potential cybersecurity incidents that could happen and how these incidents can affect users physically and mentally.

The paper is organized as follows: in the first part, there is an analysis of how the issues related to cybersecurity are treated in the specialized literature. The second part presents the potential challenges in the cybersecurity space, the main attack vectors and the security measures that can be taken, potential strategies and necessary principles that can ensure cybersecurity in the Metaverse and the user-avatar relation from the perspective of cyber safety and mental safety in Metaverse, with a particular focus on four areas: health, psychic, education and social.

RELATED WORK

Security issues in the Metaverse addressed in the specialized literature are presented from the point of view of the component technologies that create the immersive virtual experience and the cyber threats in the virtual environment that affect both users and businesses. Thus, Sun et al. (2022) address the potential security issues facing Metaverse in its current development phase using a framework organized into four layers: the interaction layer, the network layer, the application layer, and the emerging technologies layer. Tariq et al. (2023) address the security issues generated by the integration of deepfake technologies in Metaverse with an emphasis on impersonation in important application scenarios, such as virtual gaming, virtual meetings and virtual offices. A potential solution to protect avatars using digital identity verification systems is discussed. Singh & Bakar (2019) proposes a systemic architectural model of cybercrime stakeholders, whose components can be used to address the issues of policy development for global cybercrime.

Khan & Haque (2017), talk about the importance of cybersecurity in social media and present the types of cybercrimes encountered along with policies to follow. Gómez-Quintero et al. (2023) present the results of a study that identified 30 crime threats in specialized literature, which were grouped into categories regarding sexual offences, financial areas, people and property. These crimes can also appear in the Metaverse. Bhardwaj & Kaushik (2023) make a comparative analysis of security challenges in VR, AR and Metaverse technologies.

CONSIDERATIONS REGARDING CYBERSECURITY IN METAVERSE

As the emerging and immersive technologies within the Metaverse composition develop, the potential for cyber threats in the applications accessed by users will increase. According to (Shein, 2022) some cyber threats take place in the early stages of the Metaverse, and others will appear in the coming years. Following (Security, 2022), are encountered categories of threats in the Metaverse, such as: NFTs (Non-Fungible Tokens) (Gheorghe, 2023), private spaces to facilitate illegal activities or communicate with other criminals named Darkverse, financial fraud, privacy issues, cyber-physical threats, XR threats, social engineering, traditional IT attacks, other threats related to policies, environmental impact, ethics and moderation of behaviour within Metaverse.

Metaverse is characterized by the aspect of immersion and interactions between users using digital devices. Digital transactions in virtual environments are another aspect of the Metaverse. Also, the imprecise transparency of users' personal data, the multiple sources of data collection and their sharing in these virtual environments raise the issue of risks related to data.

Cybersecurity in Metaverse refers to the cybersecurity of hosting platforms and the cybersecurity of interacting users, the measures and practices that must be used to keep virtual spaces safe from potential vulnerabilities and threats.

The risks associated with cybersecurity relate to a lack of regulation, which leads to a fragmented user experience; a lack of user protection (meaning the lack of attention of digital device holders to the volume of data collected about them) and a lack of credential verification processes that also exposes users to risk.

Some key aspects of cybersecurity in Metaverse can be defined: as data protection and privacy, authentication and access control, virtual asset security, network security, secure transactions, user education, secure development practices, monitoring and incident response, regulations and compliance, and collaboration.

Cyberbullying in Metaverse refers to the use of digital tools of interaction and communication, such as social media or online platforms in virtual environments, intending to harm through harassment, threat or intimidation. It is a serious problem for people, which should not be neglected because it can have repercussions on a mental and emotional level.

According to (Pew Research Center, 2022) there are different forms of manifestation of cyberbullying, such as virtual harassment, virtual impersonation, avatar-based bullying, cyberbullying through virtual objects, virtual property theft, exclusion and isolation, virtual hate speech and discrimination.

To provide Metaverse users with safe, inclusive and enjoyable virtual environments, the cyberbullying approach requires, in addition to technological solutions, user education and user community management. Thus, important aspects such as moderation and reporting, virtual community guidelines, empowering bystanders and mental health support must be taken into account.

Cybercrimes in the Metaverse refer to criminal activities that can occur in virtual reality environments where users interact with avatars and various digital representations. The aspect of anonymity creates vulnerability in Metaverse and allows various forms of cybercrimes: virtual theft and fraud, virtual property damage, virtual currency laundering, scams and deception, malware and exploits, illegal content distribution, virtual espionage and privacy violations. According to (PWC, 2022), along with the development of areas regarding employee/customer experience, phishing cyber-attacks and social engineering scams are on the rise.

CONSIDERATIONS REGARDING CHALLENGES IN METAVERSE

General cybersecurity challenges relate to communication challenges, identity and customer vulnerabilities. Because interactions between users are based on trust, communication challenges are about better communication at scale between users (TechTarget, 2023).

Because the identity of the person users is dealing with is questionable, Metaverse users are vulnerable to identity spoofing, avatar theft, and account hacking. A big challenge for Metaverse is represented by deepfakes, which have the potential to be used in the creation of child sexual abuse material, fake news, intimidation and financial fraud. The security challenges of the VR and AR environments raise many privacy and security issues. The VR security challenges are about trust, accountability, authentication, liability, privacy, hacking and espionage, while the AR security challenges are about data integrity and physical security.

A Metaverse that cannot be trusted could also block the progress. In the study „2022 Metaverse Survey" (PWC, 2022), consisting of CEOs and consumers, both groups stated that cybersecurity and privacy are the top concerns that hold them back from adopting Metaverse.

Metaverse could enable existing cybercrime to trigger and create new types of cybercrime. A Metaverse powered by a blockchain-enabled Web3 infrastructure could be the place to find solutions, including improved protocols and cyber protection, the ability for users to control what data is shared, and better user verification. While there are many types of scams relevant to the Metaverse and the decentralized Web3 world, phishing and social engineering are some of the most prevalent.

Considering the variety and complexity of the services offered in Metaverse, there are potential incidents that must be taken into account. According to the survey (PWC, 2023) the most important potential cases of incidents refer to fraudulent messaging and social engineering, malicious airdrops and giveaways, seed phrase phishing and ice phishing.

Fraudulent messaging and social engineering methods aim to divulge private information, where scammers take the form of an avatar designed to impersonate people.

Malicious airdrops and giveaway methods are known for features such as phishing, malware distribution, unauthorized access and taking advantage of the reward approach to deceive. Seed phrase phishing methods help fraudsters take control of a victim's digital wallet and assets and make transactions on behalf of the real members. Ice phishing methods refer to assigning approval of users' cryptocurrency addresses to an attacker.

REAL CASES OF INCIDENTS IN METAVERSE

Fraudulent messaging and social engineering methods worked for the server of a Metaverse environment with transactions supported by blockchain technology that were compromised and fraudulent messages were sent to members regarding exclusive gifts. Using this method, a huge number of digital assets were extracted from the wallets of people who browsed the fake website. In this case, the Metaverse environment has been compromised.

According to (PWC, 2023), in the case of using the method named malicious airdrops and giveaway, an airdrop phishing scam carried out via social media accounts stole $1 million worth of digital assets.

In one case of seed phrase phishing, copycat sites were created for several well-known digital wallets where scammers were able to steal an important amount of money through a seed phrase phishing method. The victims are first-time users. Some mobile wallet apps may save a copy of a user's private keys, further increasing the attack surface to exploit.

Ice phishing method was used in the case of a victim that authorized a transaction and the smart contract injected with a malicious script, allowed the attacker to transact on behalf of the victim. As specified by PWC (2023), in one case, the scammers created fake websites associated with a Metaverse environment and paid for their copycat Metaverse site to appear at the top of search results. Victims linked their wallets to this site and signed a contract allowing the scammers access to their digital wallets.

Figure 1 synthesizes potential attack vectors used by fraudsters and real cases of incidents and security measures which can be taken.

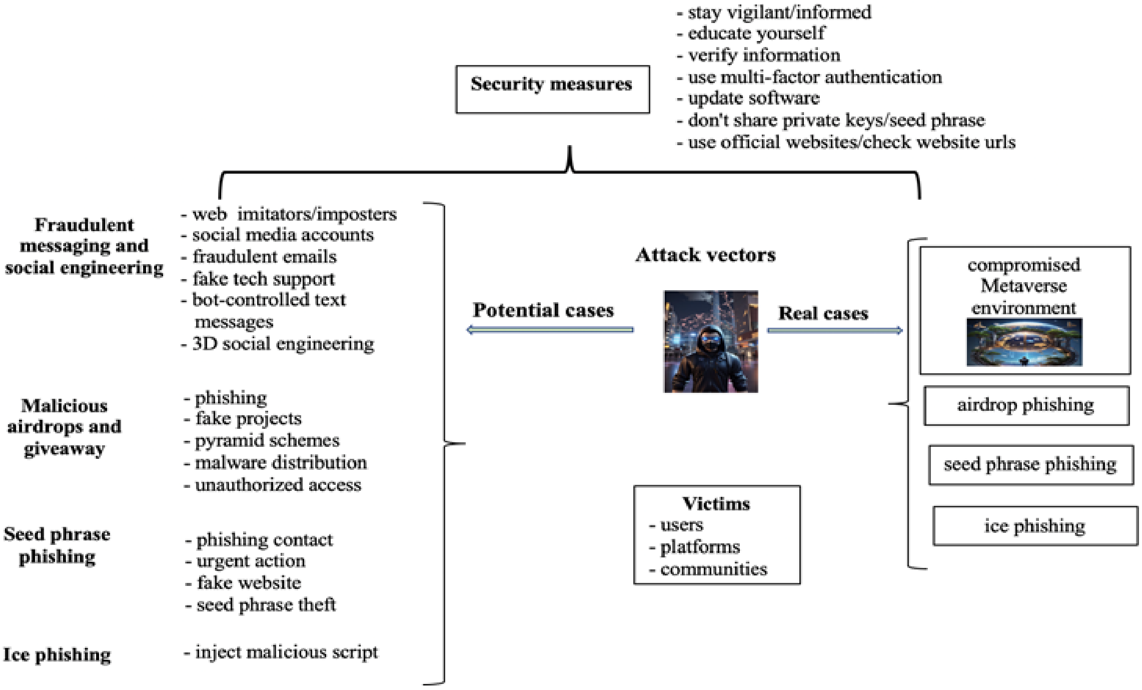


Figure 1. Attack vectors and security measures

The potential strategies and principles for ensuring cybersecurity in the Metaverse are presented in Table 1.

Table 1. Cybersecurity strategies and principles in Metaverse

Strategies and principles	Description
Encryption and Secure Communication (Canbay et al., 2022)	End-to-end encryption for data transmission and communication within the Metaverse prevents unauthorized access to sensitive information and ensures that messages cannot be intercepted and read by unauthorized users.
Multi-Factor Authentication (MFA) (Ometov et al., 2018), (PWC, 2023)	MFA adds an extra layer of security by requiring users to provide multiple forms of authentication before gaining access to their accounts and helps prevent unauthorized access even if passwords are compromised.
Virtual Asset Security (Wang et al., 2022)	Robust security measures, like secure storage mechanisms or mechanisms to report and recover stolen assets, are needed to protect users' virtual assets.
User Privacy Controls (Fernandez & Hui, 2022), (PWC, 2023)	The control over the information users share and the ability to manage their privacy settings to prevent unwanted data exposure are crucial.
Content Moderation (Hine, 2023)	It is important to use advanced content moderation tools powered by AI to identify and remove harmful or inappropriate content (such as hate speech, cyberbullying and malicious code).
Blockchain Technology (Gadekallu et al., 2022)	Integrating blockchain technology into the Metaverse can provide transparency and security for transactions, ownership, and digital identity.
Real-time Threat Detection (Morley, 2022)	AI-driven algorithms can help identify potential threats in real-time, regarding suspicious activities, such as unauthorized access attempts, or anomalies in virtual economies.
Regular Security Audits (Aks et al., 2022)	Regular security audits on Metaverse platforms are important to identify vulnerabilities, address potential weaknesses in their systems and help prevent cyberattacks before they occur.
User Education (Lin et al., 2022), (PWC, 2023)	Educating users about cybersecurity risks (such as phishing and social engineering) is crucial.
Collaboration with Security Experts (Wang et al., 2022)	Metaverse developers and companies should collaborate with cybersecurity experts to identify and address potential vulnerabilities.

BENEFITS AND RISKS IN USER-AVATAR RELATION

For the virtual world inside Metaverse, special interest is given to the fields of medicine, security, education and commerce, but concerns related to the physical and mental health of the user, privacy and socio-psychological problems remain a constant to which researchers are looking for solutions (Al-Ghaili et al., 2022).

Whether for study or entertainment, users project their real identities in the form of avatars, which serve as a facade in the Metaverse. This process can be compared to how an author inserts himself into a story, and this concept is called metalepsis (Măruță, 2023). According to Gerard Genette, a prominent French thinker who devoted an entire book to the concept of metalepsis, it refers to the deliberate manipulation of the specific causal relation linking the author to his work (Genette, 2004). Similarly, in the case of virtual reality, it connects the user to his avatar. Thus, the real user moves from his physical existence to his virtual existence and, from here, a series of benefits and risks can arise.

Avatars offer advantages such as increased social engagement, immersive educational perspectives and improved physical accessibility for people with physical disabilities (Lin et al., 2022), (Zallio & Clarkson, 2022).

Metaverse activities experienced through the avatar have the power to alleviate feelings of loneliness and isolation, creating feelings of common belonging, because there are no longer physical, spatial, social, geographical, or linguistic barriers.

A study exploring the use of Metaverse platforms for Generation Z and millennials found that Metaverse enhances social realism and presence by facilitating supportive interactions between users. Engaging in positive social interactions in the Metaverse can lead to increased relationship satisfaction and reduced feelings of loneliness. The study also found a positive relation between the number of friends and users' perceived sense of social presence in Metaverse (Oh et al., 2023).

Metaverse has the potential to transform society, connect individuals to the digital world and reduce social identity conflicts, but it can also lead to unhealthy lifestyles (BUANA, 2023). However, an excessive amount of time devoted to Metaverse could lead to negative consequences on physical and mental health, deeper levels of addiction to metaverse activities (Pew Research Center, 2022), anxiety and depression (Usmani et al., 2022). According to (Pătrășcanu, 2023), the consequences for physical health include a series of adverse effects, such as vision impairment, spatiotemporal disorientation, postural instability, physical discomfort, nausea and/or dizziness, convulsions, accidents, severe fatigue and pain head. These consequences arise from the tendency of users to ignore physical activity and self-care practices.

In addition, sharing personal information and engaging in online interactions can create privacy and security issues, exposing users to various risks such as new threats to users' personal data, identity theft and cyberbullying (Zhao et al., 2022).

Figure 2 shows the benefits and risks that may appear in the relationship between the user and his avatar, grouped into six major categories.

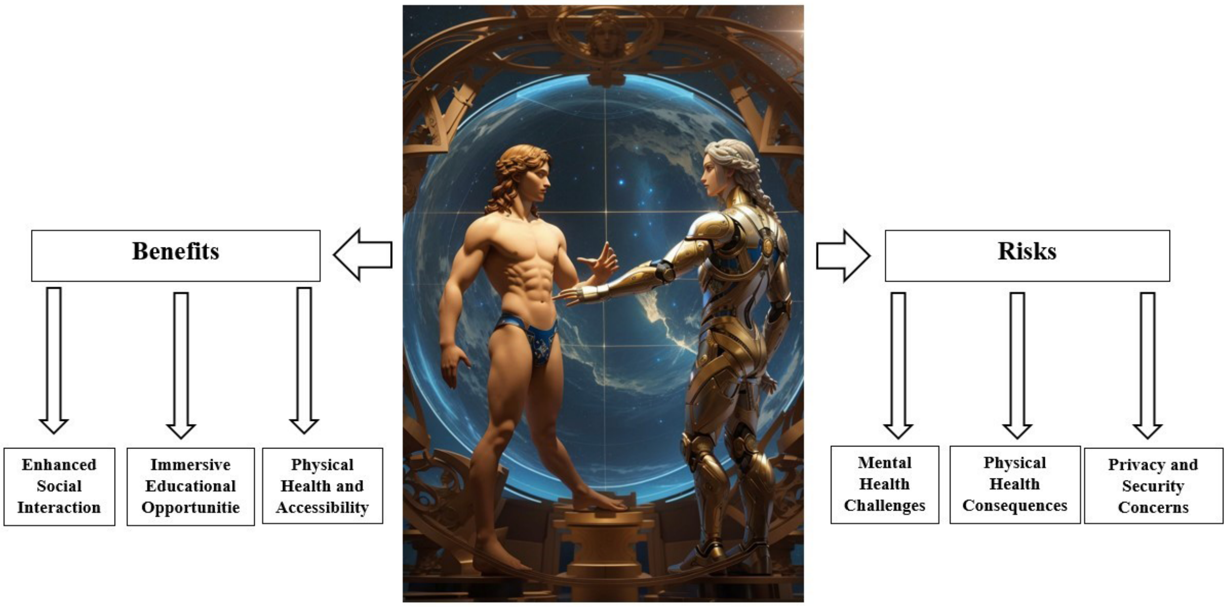

Benefits
Enhanced Social Interaction
Immersive Educational Opportunitie
Physical Health and Accessibility
Risks
Mental Health Challenges
Physical Health Consequences
Privacy and Security Concerns

Figure 2. *The impact of the Avatar on the User*

Table 2 provides a detailed description of the categories of benefits and risks for the four planes of influence, health, psyche, education and social.

Table 2. *Benefits and risks for influence plans*

Health Benefits	
Access to virtual health services (Curtis et al., 2023)	Easier and more accessible health care through online medical consultations or psychological therapy.
Creative exploration (Zhu et al., 2023)	Easier and more accessible health care through online medical consultations or psychological therapy.
Educational experiences (Stanoevska-Slabeva, 2022)	Improved cognitive skills and personal development.
Health Risks	
Impact on physical health (Pătrășcanu, 2023)	Physical health problems related to the lack of exercise, as well as vision problems, vertigo, headaches and nausea because of the sedentary lifestyle associated with avatar use in the Metaverse.
Data protection and security (Fernandez et al., 2022)	Risk of becoming a victim of cyber-attacks that can affect the user's privacy because of certain personal data exposed using an avatar.
Effects on mental health (Usmani et al., 2022)	Cognitive overload, anxiety, depression and other mental health problems because of prolonged use of the avatar in the Metaverse.

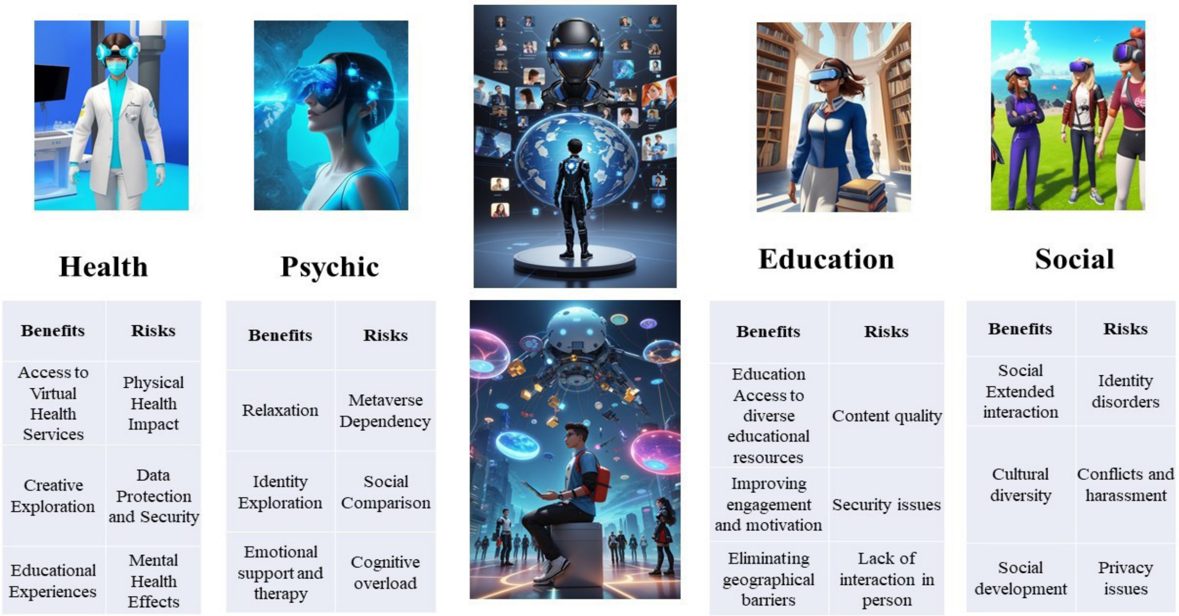
Psyche Benefits	
Relaxation (Laeeq, K., 2022)	An escape from the stress and pressures of everyday life, allowing users to relax and have fun in a virtual environment.
Identity exploration (Dudoglo & Ritter, 2022)	The opportunity to explore different aspects of identity and express creativity, can contribute to the development of a positive self-image.
Emotional support and therapy (Cerasa et al., 2022)	Online emotional support and therapy services offered by some Metaverse platforms, can help users cope with stress, anxiety or depression.
Psyche Risks	
Metaverse addiction (Bojic, 2022)	Addiction, social isolation and neglect of real-life responsibilities, with negative effects on mental health, because of the excessive use of Metaverse.
Social comparison (WAN et al., 2022)	Anxiety and stress because of unhealthy social comparisons, as users can be exposed to unrealistic standards of beauty, success or happiness.
Cognitive overload (Kim et al., 2023)	Cognitive overload and mental exhaustion due to excess stimuli, interactions and constant participation in the Metaverse.
Education Benefits	
Access to diverse educational resources (Alam & Mohanty, 2022)	Access to a wide range of educational resources provided by Metaverse and improved quality and diversity of education, such as online courses, interactive learning materials, virtual libraries and simulations.
Improving engagement and motivation (Lee et al., 2023)	Increased level of engagement and motivation in learning due to the interactions and collaboration in Metaverse with other users or participation in gamified educational experiences.
Eliminating geographical barriers (Yemenici, 2022)	Eliminating the geographical barrier and facilitating global collaboration and learning through connecting Metaverse students and teachers from long distances.
Education Risks	
Content Quality (Tlili et al., 2022)	Users are exposed to incorrect or inappropriate information for their age and education level because of the unverified or not high-quality content on Metaverse.
Security issues (Choi et al., 2022)	Vulnerability of the Metaverse to cyber-attacks or abuses, which may endanger users' personal data and privacy.
Lack of face-to-face interaction (Han et al., 2023)	A negative impact on the development of social skills and interpersonal relationships because learning in the Metaverse, may not completely replace face-to-face interactions and teacher-student relations in the physical environment.
Social Benefits	
Extensive interaction (Han et al., 2023)	Extensive opportunities to interact with people around the world, expand users' social circle, collaborate on projects or participate in virtual social events.

Cultural diversity (Lepez, 2022)	Connected users with people from different cultures and socio-economic backgrounds, allowing them to learn and experience different perspectives and traditions.
Social development (Lee et al., 2023)	The development of social skills such as communication, conflict resolution and teamwork due to social interactions in the Metaverse.
Social Risks	
Identity disorders (Usmani et al., 2022)	Confusion or the development of identity disorders, with negative impact on mental health because of the excessive exploration of identity in the Metaverse.
Conflicts and Harassment (Fernandez & Hui, 2022)	The conducive environment of the Metaverse for conflicts and harassment, as users can hide their real identity behind the avatar and act without immediate social consequences.
Privacy issues (Di Pietro & Cresci, 2021)	Exposure of personal data and privacy, and users may become victims of security breaches or abuses.

By adopting a conscious approach to the virtual world, users can effectively reap the benefits of avatars while minimizing any adverse effects on their mental, physical and social, educational health.

Using an avatar in the Metaverse can bring both benefits and risks to the user.

Figure 3 shows the four areas of major influence on users in relation to their avatar, along with the benefits and risks involved in each area.



Health

Benefits	Risks
Access to Virtual Health Services	Physical Health Impact
Creative Exploration	Data Protection and Security
Educational Experiences	Mental Health Effects

Psychic

Benefits	Risks
Relaxation	Metaverse Dependency
Identity Exploration	Social Comparison
Emotional support and therapy	Cognitive overload

Education

Benefits	Risks
Education Access to diverse educational resources	Content quality
Improving engagement and motivation	Security issues
Eliminating geographical barriers	Lack of interaction in person

Social

Benefits	Risks
Social Extended interaction	Identity disorders
Cultural diversity	Conflicts and harassment
Social development	Privacy issues

Figure 3. *Benefits and risks in the influence plans*

Metaverse users must be aware of the benefits and risks associated with the immersive experience they desire. To enjoy these benefits as much as possible, with minimal risk to their safety and health, it is important that they set clear limits on their time spent in the Metaverse, strike a balance between their time spent in real life and their time spent in the virtual world.

CONCLUSIONS

Metaverse is a technology that continues to develop and will bring along new opportunities and new cybersecurity threats that have associated new risks.

Virtual reality solutions are preferred by individual users who want enhanced immersive experiences, but also by companies looking to adopt Metaverse to grow their businesses. Immersive technologies are vulnerable and allow attackers to compromise the security of activities in the Metaverse and, at the same time they can have profound implications for the physical and mental health of connected people.

Knowing the potential cybersecurity threats in the Metaverse is an advantage as strategies can be put in place to prevent new types of threats in the future.

Connecting to the virtual environment through digital devices can have deep repercussions on the physical and mental health of individuals. Users will need to realize that as they accept the advances of the Metaverse, they must learn how to protect themselves - by following cybersecurity rules and prioritising their health and the integrity of their bodies and minds - by finding a balance between real-life and virtual-life.

ACKNOWLEDGMENT

The work presented in this paper is supported by the Core Program within the National Research Development and Innovation Plan 2022-2027, carried out with the support of MCID, project no 23380601, “Advanced research in the Metaverse and emerging technologies for the digital transformation of society”

REFERENCE LIST

Al-Ghaili, A.M., Kasim, H., Al-Hada, N.M., Hassan, Z., Othman, M., Hussain, T.J., Kasmani, R.M. & Shayea, I. (2022) A review of metaverse’s definitions, architecture, applications, challenges, issues, solutions, and future trends. In: *IEEE Access*. 10, pp. 125835 - 125866. doi: 10.1109/ACCESS.2022.3225638.

Aks, S.M.Y., Karmila, M., Givan, B., Hendratna, G., S etiawan, H.S., Putra, A.S., Winarno, S.H., Kurniawan, T.A., Simorangkir, Y.N., Taufiq, R. & Herawaty, M.T. (2022) A Review of Blockchain for Security Data Privacy with Metaverse. In: *2022 International Conference on ICT for Smart Society (ICISS)*. doi: 10.1109/ICISS55894.2022.9915055.

Alam, A. & Mohanty, A. (2022). Metaverse and Posthuman animated avatars for teaching-learning process: interperception in virtual universe for educational transformation. *Innovations in Intelligent Computing and Communications (ICIICC)*. Springer, Cham. 1737, pp. 47 - 61. doi: 10.1007/978-3-031-23233-6_4.

Analytics Insight. (28 February 2023) *Major Cybersecurity Challenges in Metaverse*. https://www.analyticsinsight.net/major-cybersecurity-challenges-in-metaverse/.

Bhardwaj, A. & Kaushik, K. (2023) Metaverse or Metaworst with Cybersecurity Attacks. *IT Professional*. 25(3), 54-60. doi: 10.1109/MITP.2023.3241445.

Bojic, L. (2022) Metaverse through the prism of power and addiction: what will happen when the virtual world becomes more attractive than reality? *European Journal of Futures Research*, 10(1), 1-24. doi: 10.1186/s40309-022-00208-4.

Buana, I.M.W. (2023) Metaverse: Threat or Opportunity for Our Social World? In understanding Metaverse on sociological context. *Journal of Metaverse.* 3(1), 28-33. doi: 10.13140/RG.2.2.27795.14885.

Canbay, Y., Utku, A. & Canbay, P. (2022) Privacy concerns and measures in metaverse: A review. In: *15th International Conference on Information Security and Cryptography (ISCTURKEY).* pp. 80-85. doi: 10.1109/ISCTURKEY56345.2022.9931866.

Cerasa, A., Gaggioli, A., Marino, F., Riva, G. &Pioggia, G. (2022) The promise of the metaverse in mental health: the new era of MEDverse. *Heliyon*. 8(11):e11762. doi: 10.1016/j.heliyon.2022.e11762.

Choi, M., Azzaoui, A.E., Singh, S.K., Salim, M.M., Jeremiah, S.R. & Park, J.H. (2022) The future of metaverse: Security issues, requirements, and solutions. *Human-Centric Computing and Information Sciences*. 12. doi: 10.22967/HCIS.2022.12.060.

Chow, Y.W., Susilo, W., Li, Y., Li, N. & Nguyen, C. (2022) Visualization and Cybersecurity in the Metaverse: A Survey. *Journal of Imaging*, 9(1), 1. doi: 10.3390/jimaging9010011.

Curtis, C. & Brolan, C.E. (2023). Health care in the metaverse. *Med J Aust*. 218 (1), 46.

Di Pietro, R. & Cresci, S. (2021) Metaverse: security and privacy issues. In: *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. IEEE. pp. 281-288. doi: 10.1109/TPSISA52974.2021.00032.

Dudoglo, A. & Ritter, F. (2022) *Avatar Selection in the Metaverse: How users choose their digital persona in VRChat.* https://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-476710.

Ene, I.E. & Savu, D. (2023) Cybersecurity - A Permanent Challenge for the Energy Sector. *Romanian Cyber Security Journal.* 5 (1), 107 - 119. doi: 10.54851/v5i1y202310.

Fernandez, C.B. & Hui, P. (2022) July. Life, the metaverse and everything: An overview of privacy, ethics, and governance in metaverse. In: *2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW).* pp. 272-277. doi: 10.1109/ICDCSW56584.2022.00058.

Gadekallu, T.R., Huynh-The, T., Wang, W., Yenduri, G., Ranaweera, P., Pham, Q.V., da Costa, D.B. & Liyanage, M. (2022) Blockchain for the metaverse: A review. *Future Generation Computer Systems*. 143, 401 - 419. doi: 10.1016/j.future.2023.02.008.

Genette, G. (2004) *Metalepse: De la figure a la fiction*. https://www.seuil.com/ouvrage/metalepse-de-la-figure-a-la-fiction-gerard-genette/9782020601306.

Gheorghe, P.N.M. (2023) Exploring the Potential of Institutional NFTs Technology in the Emerging Digital Ecosystems of Web3. *Romanian Cyber Security Journal*. 5(1), 11-22. doi: 0.54851/v5i1y202302.

Gómez-Quintero, J., Johnson, S., Borrion, H. & Lundrigan, S. (2023) *A scoping study of crime facilitated by the metaverse*. https://osf.io/preprints/socarxiv/x9vbn/.

Han, E., Miller, M.R., DeVeaux, C., Jun, H., Nowak, K.L., Hancock, J.T., Ram, N. & Bailenson, J.N. (2023) People, places, and time: a large-scale, longitudinal study of transformed avatars and environmental context in group interaction in the metaverse. *Journal of Computer-Mediated Communication*. 28(2), p.zmac031. doi: 10.1093/jcmc/zmac031.

Hine, E. (2023) Content Moderation in the Metaverse Could Be a New Frontier to Attack Freedom of Expression. *Philosophy & Technology*. 36(3), 43.

Kim, D.Y., Lee, H.K. & Chung, K. (2023) Avatar-mediated experience in the metaverse: The impact of avatar realism on user-avatar relationship. *Journal of Retailing and Consumer Services.* 73, 103382.

Khan, M. & Haque, S. (2017) Cyber Security and Ethics on Social Media. *Journal of Modern Developments in Applied Engineering & Technology Research*. 1(2), 51-58.

Laeeq, K. (2022). *Metaverse: why, how and what.* https://www.researchgate.net/publication/358505001_Metaverse_Why_How_and_What.

Lee, H.W., Chang, K., Uhm, J.P. and Owiro, E., 2023. How Avatar Identification Affects Enjoyment in the Metaverse: The Roles of Avatar Customization and Social Engagement. Cyberpsychology, Behavior, and Social Networking, 26(4), pp.255-262.

Lepez, C.O., (2022). Metaverse and education: a panoramic review. *Metaverse Basic and Applied Research*, 1, pp.2-2.

Lin, H., Wan, S., Gan, W., Chen, J. and Chao, H.C., 2022, December. Metaverse in education: Vision, opportunities, and challenges. In: *2022 IEEE International Conference on Big Data (Big Data)*. pp. 2857-2866.

Măruță, M., (2023). I*dentitatea Virtuală*, Humanitas, București

Morley, N., (2022). Image Processing Computational Algorithms, Movement and Behavior Tracking Tools, and Virtual Retail Algorithms in a Real-Time Interoperable Decentralized Metaverse. E*conomics, Management & Financial Markets*, 17(3).

Oh, H.J., Kim, J., Chang, J.J., Park, N. and Lee, S., (2023). Social benefits of living in the metaverse: The relationships among social presence, supportive interaction, social self-efficacy, and feelings of loneliness. *Computers in Human Behavior,* 139, 07498.

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T. & Koucheryavy, Y., (2018). Multi-factor authentication: A survey. *Cryptography*. 2(1), p.1.

Pătrăşcanu, S., (9 May 2023). *Metaversul: efectele universului digital*, https://www.reginamaria.ro/articole-medicale/metaversul-efectele-universului-digital.

Pew Research Center (30 June 2022) *The Metaverse in 2024*.

PWC. (2022) *PwC 2022 US Metaverse Survey.* https://www.pwc.com/us/en/tech-effect/emerging-tech/metaverse-survey.html.

PWC. (2023) *Metaverse security: Emerging scams and phishing risks.* https://www.pwc.com/us/en/tech-effect/cybersecurity/emerging-scams-and-phishing-risks-in-the-metaverse.html [Accessed 28th July 2023].

Singh, M.M. & Bakar, A.A., 2019. A systemic cybercrime stakeholders architectural model. *Procedia computer science*. 161, pp.1147-1155.

Security (10 August 2022). *9 security threats in the metaverse.* https://www.securitymagazine.com/articles/98142-9-security-threats-in-the-metaverse.

Shein, E. (8 August 2022). TechRepublic. Innovation. *The metaverse faces more than 8 potential cyberthreats.* https://www.techrepublic.com/article/the-metaverse-faces-more-than-8-potential-cyberthreats/.

Stanoevska-Slabeva, K., 2022. Opportunities and challenges of metaverse for education: a literature review. *EDULEARN22 Proceedings*, pp.10401-10410.

Sun, J., Gan, W., Chao, H.C. & Yu, P.S., 2022. Metaverse: Survey, applications, security, and opportunities. *arXiv preprint arXiv:2210.07990*.

Tariq, S., Abuadbba, A. & Moore, K., 2023. Deepfake in the Metaverse: Security Implications for Virtual Gaming, Meetings, and Offices. *arXiv preprint arXiv:2303.14612*.

TechTarget|Security (November 2023) *Top metaverse cybersecurity challenges: How to address them.* https://www.techtarget.com/searchsecurity/tip/Top-metaverse-cybersecurity-challenges-to-consider.

Tlili, A., Huang, R., Shehata, B., Liu, D., Zhao, J., Metwally, A.H.S., Wang, H., Denden, M., Bozkurt, A., Lee, L.H. & Beyoglu, D. (2022) Is Metaverse in education a blessing or a curse: a combined content and bibliometric analysis. *Smart Learning Environments*, 9(1), pp.1-31.

Usmani, S.S., Sharath, M. & Mehendale, M. (2022) Future of mental health in the metaverse. *General Psychiatry*, 35(4).

Yemenici, A. D. (2022). Entrepreneurship in the world of metaverse: virtual or real?. *Journal of Metaverse*, 2(2), 71-82.

Zallio, M & Clarkson, P.J. (2022) Designing the metaverse: A study on inclusion, diversity, equity, accessibility and safety for digital immersive environments. T*elematics and Informatics*, vol. 75, 101909.

Zhao, R., Zhang, Y., Zhu, Y., Lan, R. & Hua, Z. (2023) Metaverse: Security and Privacy Concerns. *Journal of Metaverse,* 3(2), pp.93-99.

Zhu, R. & Yi, C., (2023) Avatar design in Metaverse: the effect of avatar-user similarity in procedural and creative tasks. *Internet Research*.

WANG, J., Yao, K., Liang, J., Tan, L. & Gao, Z., (2022) From Selfie To Avatar: How Social Media Affects Self-Image Cognition And Optimization?. *Available at SSRN 4121319*.

Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T.H. & Shen, X., (2022) A survey on metaverse: Fundamentals, security, and privacy. *IEEE Communications Surveys & Tutorials*.