

# Free Guy or Bad Guy: Safety, Privacy, and Security Risks for Minors in the Metaverse and Prominent Educational Considerations

Andria Procopiou<sup>1</sup>, Andriani Piki<sup>1</sup>[0000–0003–0376–1713], Eliana Stavrou<sup>2</sup>[0000–0003–4040–4942], and Nelly Zeniou<sup>1</sup>

<sup>1</sup> University of Central Lancashire Cyprus, Larnaca, Cyprus  
{aprocopiou, apiki, nzeniou}@uclan.ac.uk

<sup>2</sup> Open University of Cyprus, Nicosia, Cyprus  
eliana.stavrou@ouc.ac.cy

**Abstract.** The opportunities online platforms and services provide to minors for socialisation, entertainment, and education are plentiful. At the same time, the emergence of the Metaverse raises concerns for minors’ security, safety, privacy, and wellbeing. This paper aims to highlight prominent threats to minors on the Internet, and how these can manifest in the Metaverse. The paper also discusses key countermeasures for mitigating these risks emphasising the need for raising awareness and developing resilience through timely, relevant, and dynamically responsive education.

**Keywords:** Metaverse · Online Safety, Security, Privacy, Trust · Social Media · Virtual Reality · Augmented Reality · Minors · Wellbeing · Education

## 1 Introduction

The Metaverse is defined as a “a perpetual and persistent multiuser environment merging physical reality with digital virtuality [enabling] multisensory interactions with virtual environments, digital objects and people [through] an interconnected web of social, networked immersive environments” [1]. The term “metaverse” was firstly introduced in the fiction novel “Snow Crash” back in 1992 [2], and is a blend of the words “meta”, which stands for transcending, and “universe”. The Metaverse is presented as a universally accessible and fully immersive environment, enabled by the convergence of key technologies including virtual, augmented, mixed, and extended reality (VR/AR/MR/XR), digital twins (DT), artificial intelligence (AI) and blockchain technology [1]. The Metaverse aims to promote rich social connections between individuals and presents opportunities for experiencing an immersive digital life. It enables seamless embodied user communications in real-time, and dynamic interactions with digital artifacts [1] and avatars [3]. Avatars form the digital representation of human users in the Metaverse, capturing and visualising each user’s behaviour (gestures,

facial expressions and movements) [4] and interactions (verbal and non-verbal communication) with other users [5], as well as with the provided services or AI-enabled agents. The Metaverse strives to offer new ways in changing, and ultimately improving, our daily and social lives through immersive experiences and meaningful interactions [8].

Despite previous attempts to create parallel life in cyberspace, such as Second Life, Fortnite, Roblox, and VRChat [6], some of the biggest technological corporations have only recently started investing on the Metaverse. Notable examples include Meta (previously Facebook), Google, Microsoft, and Apple [7]. Given the ongoing technological evolution, the realisation of the Metaverse is more evident than ever before and, inevitably, it will soon be accessible to everyone, including minors. The term "minors" refers to all individuals up to 18 years old, including children (up to 12 years old) and teenagers (13-18 years old) [13]. The cognitive and maturity differences between these two age groups are significant, with minors in the age group of 11-18 years being reported as the ones who make the most conscious usage of the Internet [12]. In the near future, the Metaverse will form a state-of-the-art tool for their education [9], entertainment [10], and health-related matters [11]. Therefore, the threats and risks concerning minors are more alarming than ever before.

During the Internet 2.0 era, children became more vulnerable and easily targeted by all kinds of abusive, illegal, harmful and unacceptable behaviour [12]. Increasingly, the effective protection of minors from such threats is an open and multifaceted challenge due to the complexity of the current state of the Internet, the enormous size of its infrastructure, the explosion of the user space, and the opportunity for nearly-complete anonymity. Unfortunately, with the rise of the Metaverse, these threats are bound to be magnified due to the increased immersion level of high-fidelity VR environments [1]. Therefore, it is only a matter of time before the Metaverse becomes an extremely dangerous place for minors. Therefore, this group of users should get the highest priority when it comes to security, privacy, safety, and trust in the Metaverse.

The aim of this paper is to discuss the most notable and serious threats and risks observed in Internet 2.0 and how these can manifest in the Metaverse, focusing specifically on minors. Subsequently, we suggest possible countermeasures for protecting minors in the Metaverse, emphasising the genuine need to establish the Metaverse as an open, safe, and accessible space - a need that can only be met with properly educating minors and key stakeholders, alongside establishing proper security and safety policies.

## 2 Threats to Minors on the Internet

Undoubtedly, the Internet can pose multiple risks and threats to minors, regardless of their age group and digital literacy. Although there are no universally-accepted definitions, in the context of this paper we provide brief explanations of these threats based on relevant literature [14], before proceeding to discuss how each of these may manifest in the Metaverse.

## 2.1 Cyberbullying and Cyberharassment

Cyberbullying is "the willful and repeated harm inflicted through the use of computers" or other electronic devices [15]. Most cyberbullying acts occur on social media, chat rooms, or discussion forums. In fact, cyberbullying constitutes one of the biggest threats that social networks can pose. Adolescents share photos, videos, personal, contact, and location information (e.g., age, phone number, school, and location) on social media, to a much greater extent compared to the past. Sharing personal and sensitive information constitutes the main reason triggering cyberbullying of minors through social networks [12]. In recent years more than three million children have undergone cyberbullying in various forms, ranging from harassment to threats, while a high percentage (95%) reported that they have been victims of cyberbullying on Facebook [12].

Cyberbullying is more dominating compared to bullying occurring in physical space. Firstly, cyberbullying acts can occur at any time and place. There are no safe or "bulletproof" cyberspaces. Hence, individuals can become victims even while they are at home. Secondly, cyberbullying can reach large audiences in a very short amount of time. Furthermore, cyberbullying can transpire in a completely anonymous way, with offenders hiding behind aliases, fake profiles or fake accounts [12]. Therefore, it is significantly more difficult to effectively detect and mitigate acts of bullying in cyberspace.

When an adult performs an act of bullying online, this is classified as cyberharassment [16]. Such an act denotes harassment of individuals or groups through hateful, threatening, abusive, and offensive online messages, comments, or emails [18]. Examples of cyberharassment manifestation include, but are not limited to, receiving unwanted content (in any form, including text, photos, and videos) online; receiving offensive, inappropriate, or abusive advances on social media, chat rooms or forums; receiving threats of physical, emotional, mental, or sexual violence online; and receiving hateful, insulting and/or threatening messages, comments or emails that directly attack an individual's or a group's beliefs, preferences and identity characteristics (such as ethnic race, nationality, religion, sexual orientation, gender identification, political beliefs, financial status and personal interests, amongst others) [19].

## 2.2 Online Stalking

Online stalking encompasses all actions and behaviour that exploit the Internet or other electronic or digital means to stalk and prey upon individuals, aiming to control, intimidate or negatively influence them [20]. Like cyberbullying, cyberstalking can be conducted more easily compared to its physical counterpart, due to the anonymity the Internet offers. Cyberstalking can be part of a physical stalking act or can be solely manifested online.

## 2.3 Online Predators

Online predators are defined as the individuals who adopt "a communication process by which they apply affinity seeking strategies, while simultaneously

engaging in sexual desensitization and information acquisition about targeted victims in order to develop relationships that result in need fulfillment such as physical sexual solicitation” in cyberspace [21]. They exploit the minors’ naive nature and vulnerabilities [12].

## 2.4 Online Gambling

Online gambling encompasses all virtual gambling games in cyberspace. Examples include virtual bingo, slots and casino games [23]. Unfortunately, underage online gambling is a critical issue in today’s world that only keeps growing [24]. Furthermore, minors could incur a huge cost to their families while playing online games. More specifically, young players may spend considerable amounts of money to purchase virtual characters or other game features, or by just paying for subscriptions [12].

## 2.5 Illegal, Inappropriate, and Harmful Content

Minors can come across various types of ”unacceptable” content online [12]. Such content can be categorised as illegal, harmful, or age inappropriate advice. Illegal content refers to all content which is unlawful to be published online, such as footage of real or simulated crimes. Harmful advice content denotes all content which glorifies problematic behaviour and promotes minors into the adaption of such behaviour. Examples include the consumption of alcohol, drugs and other substances, committing suicide, participation in dangerous activities and challenges [22], or adoption of extreme nutritional customs. Inappropriate content denotes all content that, although not illegal, is dangerous to the minors’ development, health, and wellbeing. Examples include pornographic content and content promoting violent behaviours.

## 2.6 Social Engineering and Identity Theft

Identity theft involves any form of illegal activity aiming to obtain personal information from individuals in cyberspace [25], and it is often materialised through social engineering attacks [26]. Social engineering aims to exploit the human nature and trust that someone places to situations or another person by manipulating them to divulge confidential information. In turn, all the illegally obtained information collected is used to commit various acts of identity fraud. Examples include opening bank accounts, taking over phone contracts, and obtaining genuine and legal documents such as passports [30].

Social engineering attacks can be launched during face-to-face interactions, through the phone, or through digital means [27], with email being the typical attack channel for phishing attacks [28]. Minors are often susceptible to phishing attacks [29] due to their curiosity, naivety, and lack of awareness and education, revealing sensitive information to third parties that could lead to identity theft, and, subsequently, to accounts being compromised. Social engineering can also

enable online predators to launch other malicious activities, such as cyberharassment, leading to minors' victimisation. Minors are typically at risk through their social media accounts. There are also alternative attack vectors, such as interacting with a smart toy, an educational application (e.g., ClassDojo) or their parents' social media accounts [31]. Therefore, raising awareness and educating minors, teachers, and parents about the imminent threats, risks, and their consequences, in a timely and orchestrated manner, is imperative.

### 3 Threats to Minors in the Metaverse

The range of looming threats and the severity of their consequences become more prevalent as emerging technologies expand in all areas of social life. In this section, we discuss how the most notable threats can manifest in the Metaverse and under what circumstances.

#### 3.1 Bullying, Harassment, and Assault in the Metaverse

Cyberbullying and online harassment have proved to be extremely dangerous. Real world cases report on victims suffering from mental health deterioration, which subsequently resulted into successful suicide attempts [32]. In the Metaverse, this type of behaviour may have a serious impact due to the immersive environment. High-fidelity VR environments and violent representations in the Metaverse can trigger traumatic experiences [1]. Victims will be targets of insults and invective, verbal abuse, discriminating, racist and/or homophobic slurs, threats of violence and other forms of harassing behaviour [33]. Moreover, due to the VR/AR technologies used, these acts will impact the victims emotionally, psychologically, and physiologically. Specifically, due to avatars' sophisticated and photorealistic design, including the detailed facial expressions and body movements, the victims may endure a similar impact to a bullying/harassment scenario happening in the real world [4], hence experiencing fear, intimidation, and helplessness.

Due to the presence of open virtual "social spaces" in the Metaverse [34], potential victims are much easier to be identified and harassed and/or bullied. While in cyberbullying/online harassment occurring in social media, forums, or chatrooms, the target has the opportunity to "get away" by turning their device off, in the Metaverse, the victims are directly accessible, easier to find, and it is harder for them to escape as they can be followed by their harassers. Furthermore, the Metaverse offers the opportunity for the users to create their own content, their own metaverse-esque spaces, and personalise their avatars' appearance to offend, insult, mock, troll, and dehumanise individuals and groups. Examples include changing their skin color (e.g., "blackface") [38]. In the context of bullying and harassment, aggressors may wear clothing or accessories with biased, discriminating and overly offensive slogans or images [39], or recreate or modify the metaverse-esque spaces with posters, street wall graffiti, flags and banners which are classified as racist, homophobic, transphobic and offensive [37].

### 3.2 Stalking in the Metaverse

In the Metaverse, stalking may manifest in several ways. It will be possible to buy land and subsequently build houses in the Metaverse [35]. Therefore users' "metaverse house address" could be revealed if their harassers systematically stalk them in the Metaverse. While some social media platforms allow users to check who has viewed their profile, currently VR technologies do not allow users to be fully aware of their surroundings [4] or be aware of who might be following them or accessing their Metaverse spaces. Furthermore, the harassers may vandalise their property, stalk them in metaverse-time and even assault them. Even though the victims may not suffer any physical injuries, the psychosomatic consequences of such a traumatic experience will certainly occur and be enhanced due to the usage of immersive technologies such as VR/AR/MR/XR [36].

### 3.3 Predators and Sexual Exploitation in the Metaverse

Perhaps the most critical concern in the Metaverse for minors is the possibility of their sexual exploitation and grooming from predators who may be present under various disguises. Public spaces will be a reality in the Metaverse, where everyone will be free to socialise with users they already know, but also meet and interact with strangers [45]. Predators may easily "hide" behind avatars that have no connection to their real age or gender. Hence, they could easily pose as peers with the aim to approach minors.

Unfortunately, numerous incidents of sexual assault and violence have been reported [46], while at the same time victims of such incidents are eager to approach other victims to reveal they had similar experiences in the Metaverse. Despite the realisation of a personal boundary system (which prevents users from touching another user's avatar or getting too close to them), predators will force others to turn it off. If users fall in the predators' trap, they face the risk of being victimised, and experience any of the previously discussed behaviours [47]. Based on the incidents being reported thus far, it seems that the possibility of such exploitation is prevalent. In such cases, the associated risks are even higher for minors. Due to the immersive experience feeling more real than ever, the impact of such incidents on minors' development, mental health, and wellbeing will be shattering [36], [?].

### 3.4 Metaverse Gambling

The current technologies for the Metaverse already offer a plethora of gaming hubs, so it is only a matter of time before casinos make their appearance [40]. Currently, online gambling is prohibited for minors. However, underage users can easily bypass any security countermeasures and protocols, enter the Metaverse as adults and, in turn, gain access to casinos and participate in gambling games. This can have catastrophic consequences. First, online gambling can become alarmingly addictive for minors [42]. Opponents may exercise peer pressure to minors or challenge them to continue playing. Therefore, minors

can quickly and easily become addicted to gambling in the Metaverse [43], [44]. Secondly, due to the immersion factor as well as due to pressure from other players, minors may find it more difficult to escape from unwanted or dangerous situations. Thirdly, studies exploring the reasoning behind minors addiction to online gambling, suggest that prevalence, visibility, and glamour are the main motivations [42]. Minors seem to consider online gambling as an enjoyable and thrilling activity which allows them to win fast money [42]. It is inevitable for such emotions to be magnified through the Metaverse’s immersive environment. The Metaverse and its components are designed to offer experiences very similar to the real-world respective ones, with the usage of immersive technologies (VR/AR/MR/XR), AI-enabled agents and services, and highly-detailed virtual environments. Another key concern, is that the Metaverse’s mechanisms for protecting an individual’s identity in the real world, including their age and gender, may be exploited by players who may hide behind their unidentifiable avatars to exercise pressure against other users, including minors who many not have the resilience or stamina to escape.

### 3.5 Illegal, Inappropriate, and Harmful Content in the Metaverse

Since the Metaverse presents the means for crafting a parallel reality to users’ lives, all illegal, inappropriate and harmful content, previously observed in social encounters, social media, forums, or chat rooms, is increasingly likely to make an appearance in the Metaverse. The most important difference is that minors can be fully exposed and witness such incidents and not just watch footage of them. Examples of illegal behaviour in the Metaverse would include minors witnessing a crime, such as a murder, rape, or assault [48]. Due to the Metaverse’s realistic and immersive nature, minors are likely to suffer a significant emotional, psychological, and physiological impact from witnessing such a traumatic experience, higher than when they experience such an exposure in Internet 2.0, and similar to experiencing such an act in the real world [49]. In addition, in the case of a murder occurrence in the metaverse, the victim will potentially ”come back to life”. This is likely to confuse minors, especially the younger ones, as to the actual consequences of physically harming someone in the real world as well.

Additional examples of possible age-inappropriate exposure in the Metaverse would mainly include minors witnessing pornographic content, public indecency incidents, bullying and harassing incidents, as well as other episodes of violence. It is also possible that the avatars minors use might not necessarily correspond to their actual age, hence increasing the risks they may face. Currently, there is no certain way of ensuring that a user has specified their legal age when joining the Metaverse. Therefore, minors may freely enter virtual strip clubs or engage in other age-inappropriate activities [50]. In addition, avatars may be involved in such activities publicly, so it is possible for minors to witness these incidents while navigating the Metaverse [51], [50].

Finally, cases of harmful advice in the Metaverse are equally dangerous. Minors could be instantly offered virtual drugs, alcohol, cigarettes or other substances from peers or older users. Peer pressure, curiosity, and excitement are

common reasons why such cases materialise. Even if this does not translate to suffering any physical consequences directly, such experiences can have a critical influence on minors, and may evolve into actions, beliefs, and addictions in the physical world. As a result, they are likely to be negatively influenced to try out such substances in the real world with greater ease, since they have already done it in the Metaverse.

### 3.6 Social Engineering and Identity Theft in the Metaverse

In the Metaverse, identity theft does not merely involve stealing private and confidential information about users. Rather, it involves stealing the actual identity of the users. Specifically, facial characteristics, body movements, or even the entire avatars could be "stolen" by other users. This could be done in an attempt to gain multiple illegal or unethical benefits in the Metaverse, access restricted areas, as well as deceive minors by posing as their peers. This can prove to be particularly dangerous when it comes to predatory behaviour as already discussed.

Related to data ethics, AI algorithms and deep learning techniques can be utilised to create VR deep fake avatars and launch identity theft attacks in the Metaverse [1]. Online predators can also profile a minor through social engineering attacks employed in the Metaverse, with a focus on in-person attacks delivered through avatars. These attacks are easier to deploy compared to real-life, face-to-face social engineering attacks, since it is easier to approach minors in the Metaverse, as guardians may not enforce any controls due to lack of understanding of the environment, or failure to realise the dimensions of the threats that the Metaverse might give rise to. Due to this possibility, online predators might direct their efforts on identifying and targeting minors while socialising in the Metaverse's public spaces. This further illuminates the need for raising awareness and educating both minors and adults.

Additionally, minors could be approached by adult users that have a malicious intent in an attempt to make them reveal personal information about their Metaverse lives or real lives through "casual conversation". The adult users could even "eavesdrop" their conversations so they can learn more about them and make their encounters more effective [4]. Examples of such personal information include physical, medical, physiological, economic, cultural, or social status in the real world [52]. Also, private information regarding their behaviour, such as habits, activities and hobbies on and off the Metaverse could be obtained, enabling online predators to profile them more easily [52]. This could have a serious impact on minors and their lives, especially in the real world, as their identity could be revealed under such scenarios, further impacting their emotional and mental wellbeing.

## 4 Education and Awareness as a Countermeasure

Undoubtedly, the Metaverse will not be fully deployed overnight. It will rather be a gradual ongoing process. Still, protective measures should already start be-

ing developed and new regulations and policies should be introduced, tailored specifically for the Metaverse. Such regulations should clearly define what is considered ethical, lawful, and acceptable behaviour in the Metaverse as well as what the consequence will be when these regulations are violated [53], [54]. From a technological perspective, appropriate and effective content moderation, filtering and reporting mechanisms should be developed [55]. From a governmental and policy making perspective, it is essential to disseminate and enforce the necessary policies and procedures at different levels (public, educational institutions, business organisations). However, perhaps the most important and meaningful countermeasure that should be of the highest priority is educating the minors themselves about the Metaverse and the potential dangers looming ahead, as well as how they should recognise such dangers, avoid them, and successfully report them. It is imperative for young users to be educated and prepared for any potential incidents which may be regarded as ominous or worrying, but also to be supported through open discussions with adults and experts at family, school, and community level [56]. Therefore, from an educational perspective, raising awareness and developing students' knowledge, skills, and resilience, sets the cornerstone for a safer and more secure future.

#### 4.1 Frameworks for Addressing Safety, Privacy, and Security Risks

Various frameworks have been proposed for raising cybersecurity awareness in various contexts. Examples include a framework for improving security awareness in organisational contexts, a cybersecurity awareness and education framework developed to assist in creating a cyber-secure culture among Internet users, a conceptual framework for the design and implementation of cybersecurity games to improve cybersecurity education and pedagogical effectiveness using game-based approaches, and a cybersecurity awareness framework for academia [67], amongst others. However, there is a lack of conceptual frameworks focusing specifically on minors.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework [57] is a generic, flexible, and technology neutral model which can serve as a foundation towards formulating a concrete approach for addressing safety, privacy, and security risks that minors may face in the Metaverse. NIST Cybersecurity Framework specifies five functional areas to manage threats: identify, protect, detect, respond, and recover. Taking these areas into consideration, appropriate awareness-raising and educational activities should be designed, developed, and implemented, focusing on Metaverse usage by minors. The objective should be to build knowledge and skills so that minors can:

- Understand the technologies utilised in the Metaverse and the relevant risks.
- Develop critical thinking skills as to how an online predator might try to exploit them in an immersive environment, and be in position to recognise such an intention and successfully escape.
- Realise how someone with a malicious intent can collect information and exploit it to profile minors and lure them into a harmful situation, both physically and mentally.

- Stand up in case of a harmful/offensive situation and have the confidence, resilience, and knowledge to report it to the appropriate authority.

In addition to educating and upskilling minors themselves, other relevant stakeholders and communities, such as parents and educators, should also be trained and informed [51], so they can understand what the Metaverse environment implies, appreciate the associated threats and risks, offer support and guidance, and liaise with appropriate authorities to report incidents and seek further support, when needed. Such knowledge and skills can promote the development of a cyber-resilience culture [58] which will empower Metaverse users to predict, detect, and respond to threats, contributing to a global cyber-resilient society.

## 4.2 Gamification and Game-Based Learning Approaches to Education

Games have been used as learning tools for ages and playing games constitutes one of the fundamental ways to learn. Therefore, games constitute an avenue towards addressing and responding to prominent educational and training needs. Such efforts can utilise game-based learning (GBL) strategies [59], serious games [60], gamification techniques, and emerging immersive technologies including the Metaverse itself [61], to raise cybersecurity awareness, and increase minors' and adults' familiarity with core safety, privacy, and security concepts pertinent to the Metaverse.

Various serious games and gamification efforts have been employed to address cybersecurity-oriented educational needs, adopting a range of game genres to engage, motivate, and educate learners [60, ?, ?]. The Cybersecurity & Infrastructure Security Agency (CISA) [71] developed a series of educational cybersecurity games available on mobile devices for adults and children. Each game presents simulated cybersecurity threats, defenses, and response actions. For instance, "Defend the Crown" encourages players to develop and apply a basic understanding of attacks and defense strategies over three challenging stages and 18 levels, while "Hotel Hijinks" is a mobile game which focuses specifically on providing learning materials to high school students related to the Internet of Things (IoT), the cybersecurity challenges posed by it, and cyber safety in a fun and interactive way, and it is available on both iPhone and Android devices. While the intended audience is high school students, this mobile game is available for anyone interested to develop their knowledge on these topics [71].

Other examples of games in the broader field of cybersecurity include: "Operation Digital Ant", a team-based competitive game aiming to familiarise players with different types of insider motives and attacks, and raise their awareness on security countermeasures while advancing through collaborative scenarios and role-play [63]; "AIT Cyber Range", a virtual simulation environment aiming to increase the users' preparedness and dexterity by training them to identify and mitigate various incidents and attacks [64]; and "CyberCEIGE", a video game

that teaches professional staff and students computer and network security concepts and the impact of decision making on physical, hardware, software, and user security, using real life scenarios [68], amongst other educational games. The available games feature various levels which must be completed to unlock subsequent levels or scenarios, and adopt dynamic complexities that adjust based on the players' performance, level of expertise, time allocated to complete a task, and other game features [67]. Such GBL approaches can be used for the education of various target groups, such as students, parents, teachers, school leaders, employees at local public authorities, professional and non-professional staff, and others. These target groups can be trained through playing educational games aiming to improve their digital skills and strengthen their own resilience and decision making, in terms of security, privacy, and safety, as well as the overall cyber-resilience of their organisations [66].

Further to GBL, employing gamification techniques and game-like features (such as interactivity, instant feedback, progress indicators, time limits, unveiling of levels, scoreboards, badges and awards) can also be instrumental for achieving the learning objectives, that is to raise security, safety, and privacy awareness. Gamification in the field of cybersecurity typically involves real-life scenarios with a focus on detecting and handling cybersecurity attacks, and incident response procedures that must be followed in the event of a cybersecurity threat [67], [69]. Scenario-based learning, problem-based learning, or case-based learning when employed in a gamified or GBL context, support active learning strategies and increase learner engagement by immersing them in learning experiences using interactive scenarios. In such approaches, participants must apply their subject knowledge, critical thinking, and problem solving skills to solve multiple question by working their way through a story line or narrative that is usually based on an ill-structured or complex problem [70]. Another area of employing gamification in cybersecurity education, is through revealing vulnerabilities of the user's own work environment by generating game data based on automated IT-security analysis of installed apps on the user's smartphone [65].

An important consideration for the successful use of novel serious games and game-based pedagogical approaches, is to ensure they are adapted to specific age groups and context of learning. They need to be accessible, inclusive, and properly designed to promote users' upskilling, critical thinking, wellbeing, and ability to respond to Metaverse-related risks and threats. Recent educational efforts adopt an enthralling twofold strategy towards increasing students' cybersecurity awareness while, simultaneously, motivating students to pursue cybersecurity as a career, by employing game-based strategies [59]. While such approaches may be effective for older students, younger users need a more playful approach, so they can learn through play, and test the impact of their decision making process in a safe environment, through trial and error, repetitions, and simulated interactions, before consciously entering a dynamic and complex environment such as the Metaverse.

Undeniably, the Metaverse environment itself can add a new dimension to the field of educational technologies [61] addressing the educational and training

needs of both minors and adults. Applications of "Meta-Education" have already shown spectacular results in terms of training speed, performance, and retention [1]. Nevertheless, the underlying technologies, architecture, and infrastructure of the Metaverse have not yet matured. Therefore, it is considered a necessity to determine appropriate strategies for the use of Metaverse in education [61], especially when educating minors. At the same time, it is essential for scientists and educators to continue pursuing an in-depth understanding of the Metaverse's widespread impact on the safety, privacy, health, and security risks it can have on users.

## 5 Conclusion

This paper discusses the dangers and risks the Metaverse can pose to minors. Undeniably, individuals belonging to such age groups spend a considerable amount of time online. Therefore, it is expected for them to shift to the Metaverse, as soon as it becomes widely accessible. Unfortunately, this unleashes a plethora of threats and risks, with varying degrees of severity and impact on their security, privacy, online and offline safety, mental health and wellbeing. Alongside the immersive features the Metaverse encapsulates for providing an enhanced, rich, holistic experience of a parallel world, it also contributes to the magnification of the psychological impact and negative experiences that may occur in such a multiuser, universally accessible, embodied context. Extremists, terrorists, predators, and criminals are likely to be fully aware of the capabilities the Metaverse can provide them with, and may exploit these to maximise their efforts in radicalising individuals, recruiting new members, spreading their propaganda, effectively planning attacks both in the physical and virtual space and finding new targets more accessibly in the virtual world. Regardless of the legislation, standards, regulations and policies, guidelines and protective countermeasures that shall be developed in the years to come to render the Metaverse an open, accessible space, it is unlikely that it will ever be an absolutely safe, inclusive, and secure space. Therefore, the timely and ongoing education, awareness, and upskilling of minors and all key stakeholders, constitute key priorities.

## References

1. S. Mystakidis. 2022. Metaverse. Encyclopedia (Basel, 2021) 2, 1 (2022), 486–497. doi:<https://doi.org/10.3390/encyclopedia2010031>
2. J. Joshua, "Information bodies: Computational anxiety in Neal Stephenson's Snow Crash," *Interdiscip. Lit. Stud.*, vol. 19, no. 1, pp. 17–47, 2017.
3. C. Lacey and C. Caudwell, "Cuteness as a 'Dark Pattern' in Home Robots," 2019 14th ACM/IEEE International Conference on Human-Robot Interaction (HRI), 2019, pp. 374–381, doi: 10.1109/HRI.2019.8673274.
4. L.-H. Lee et al., "All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda," *arXiv [cs.CY]*, 2021.

5. A. Davis et al., "Avatars, people, and virtual worlds: Foundations for research in metaverses," *J. Assoc. Inf. Syst.*, vol. 10, no. 2, pp. 90–117, 2009.
6. Y. K. Dwivedi et al., "metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy," *Int. J. Inf. Manage.*, vol. 66, no. 102542, p. 102542, 2022.
7. J. Maganis, "Top companies building in the metaverse," Crowdcreate, 27-Apr-2022.
8. E. Dincelli and A. Yayla, "Immersive virtual reality in the age of the metaverse: A hybrid-narrative review based on the technology affordance perspective," *J. Strat. Inf. Syst.*, vol. 31, no. 2, p. 101717, 2022.
9. K. Hirsh-Pasek, J. M. Zosh, H. S. Hadani, R. M. Golinkoff, K. Clark, C. Donohue, and E. Wartella, "A whole new world: Education meets the metaverse," Report, 2002, [Online] Available: <https://www.brookings.edu/research/a-whole-new-world-education-meets-the-metaverse>
10. C. Kerdvibulvech. 2022. Exploring the impacts of COVID-19 on digital and metaverse games. In *Communications in Computer and Information Science*. Springer International Publishing, Cham, 561–565.
11. L. Petrigna and G. Musumeci. 2022. The metaverse: A new challenge for the healthcare system: A scoping review. *J. Funct. Morphol. Kinesiol.* 7, 3 (2022), 63. doi:<https://doi.org/10.3390/jfmk7030063>
12. A. Tsirtsis, N. Tsapatsoulis, M. Stamatelatos, K. Papadamou and M. Sirivianos, "Cyber security risks for minors: A taxonomy and a software architecture," 2016 11th International Workshop on Semantic and Social Media Adaptation and Personalization (SMAP), Thessaloniki, Greece, 2016, pp. 93-99, doi: 10.1109/SMAP.2016.7753391.
13. ITU, 2020. "Guidelines for children on child online protection", [Online] Available: <https://www.itu-cop-guidelines.com>
14. Nidirect, 2015. "Social media, online gaming and keeping children safe online". [Online] Available: <https://www.nidirect.gov.uk/articles/social-media-online-gaming-and-keeping-children-safe-online>
15. Cyberbullying Research Center. "What is cyberbullying?" Cyberbullying Research Center. [Online] Available: <https://cyberbullying.org/what-is-cyberbullying>
16. R. Slonje, P. K. Smith, and A. Frisé, "The nature of cyberbullying, and strategies for prevention," *Comput. Human Behav.*, vol. 29, no. 1, pp. 26–32, 2013.
17. F. Stevens, J. R. C. Nurse, and B. Arief, "Cyber stalking, cyber harassment, and adult mental health: A systematic review," *Cyberpsychol. Behav. Soc. Netw.*, vol. 24, no. 6, pp. 367–376, 2021.
18. US Legal, Inc. Cyber harassment law and legal definition. Uslegal.com. [Online] Available: <https://definitions.uslegal.com/c/cyber-harassment>
19. Cyber harassment. European Institute for Gender Equality. [Online] Available: <https://eige.europa.eu/thesaurus/terms/1486>
20. M. L. 2007. "Pittaro. Cyber stalking: An Analysis of Online Harassment and Intimidation," *Cybercrimejournal.com*. [Online] Available: <https://www.cybercrimejournal.com/pdf/mpittarojccjuly2007.pdf>
21. C. H. Ngejane, G. Mabuza-Hocquet, J. H. P. Eloff, and S. Lefophane. 2018. Mitigating online sexual grooming cybercrime on social media using machine learning: A desktop survey. In *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)*, IEEE, 1–6.
22. Q. Nguyen. 2021. "Don't let your kids try these 9 dangerous TikTok trends". CyberPurify. [Online] Available: <https://cyberpurify.com/knowledge/9-dangerous-tiktok-trends>

23. LawInsider. Online gambling definition. [Online] Available: <https://www.lawinsider.com/dictionary/online-gambling>
24. P. Gómez, S. Feijóo, T. Braña, J. Varela, and A. Rial, "Minors and online gambling: Prevalence and related variables," *J. Gambl. Stud.*, vol. 36, no. 3, pp. 735–745, 2020.
25. D. S. Wall. 2013. Future Identities: Changing identities in the UK -the next 10 years DR 19: Identity Related Crime in the UK. Gov.uk. Retrieved December 31, 2022
26. H. Aldawood and G. Skinner, "Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review," 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), Wollongong, NSW, Australia, 2018, pp. 62–68, doi: 10.1109/TALE.2018.8615162.
27. H. Aldawood and G. Skinner, "A taxonomy for social engineering attacks via personal devices," *Int. J. Comput. Appl.*, vol. 178, no. 50, pp. 19–26, 2019.
28. K. Ivaturi, L. Janczewski, "A Taxonomy for Social Engineering attacks," *CONF-IRM 2011 Proceedings*, pp. 2–11, 2011.
29. J. Nicholson, Y. Javed, M. Dixon, L. Coventry, O. D. Ajayi and P. Anderson, "Investigating Teenagers' Ability to Detect Phishing Messages," *IEEE European Symposium on Security and Privacy Workshops*, 2020, pp. 140–149, doi: 10.1109/EuroSPW51379.2020.00027
30. Police.uk, "Identity fraud and identity theft", [Online] Available: <https://www.actionfraud.police.uk/a-z-of-fraud/identity-fraud-and-identity-theft>
31. Internet Matters. 2019. "Learn about privacy and identity theft". [Online] Available: <https://www.internetmatters.org/issues/privacy-identity/learn-about-privacy-and-identity-theft>
32. A. Ingham. 2018. 7 real life cyberbullying horror stories. Family Orbit Blog. [Online] Available: <https://www.familyorbit.com/blog/real-life-cyberbullying-horror-stories>
33. Maritsa Georgiou. 2022. Harassment still exists in the metaverse, even for kids. Newsy. [Online] Available: <https://www.newsly.com/stories/harassment-still-exists-in-the-metaverse-even-for-kids>
34. M-C. Florian. 2022. Can Public Space be Created in the metaverse? ArchDaily. [Online] Available: <https://www.archdaily.com/987613/can-public-space-be-created-in-the-metaverse>
35. B. Marr. 2022. How to buy land and real estate in the metaverse. Forbes. [Online] Available: <https://www.forbes.com/sites/bernardmarr/2022/03/23/how-to-buy-land-real-estate-in-the-metaverse>
36. S. Frenkel and K. Browning. 2021. The metaverse's dark side: Here come harassment and assaults. The New York times. [Online] Available: <https://www.nytimes.com/2021/12/30/technology/metaverse-harassment-assaults.htm>
37. A. Procopiou, "Ready Player Bad: The Future Rise of Extremism and Terrorism in the Metaverse," 2022 IEEE 2nd International Conference on Intelligent Reality (ICIR), Piscataway, NJ, USA, 2022, pp. 31–34, doi: 10.1109/ICIR55739.2022.00022
38. M. Sommer. (2020). "How ELSE are you supposed to dress up like a Black Guy?": negotiating accusations of Blackface in online newspaper comments. *Ethnic and Racial Studies*, 43(16), 57–75.
39. S. Ozalp, M. L. Williams, P. Burnap, H. Liu, and M. Mostafa, "Antisemitism on Twitter: Collective efficacy and the role of community organisations in challenging online hate speech," *Soc. Media Soc.*, vol. 6, no. 2, p. 205630512091685, 2020.

40. Neva. 2022. How will the metaverse change online gambling? 800gambler.org. [Online] Available: from <https://800gambler.org/how-will-the-metaverse-change-online-gambling>
41. A. Rial, S. Golpe, M. Isorna, T. Braña, and P. Gómez, “Minors and problematic Internet use: Evidence for better prevention,” *Comput. Human Behav.*, vol. 87, pp. 140–145, 2018.
42. Webroot.com. Internet gambling among teens and college students. [Online] Available: <https://www.webroot.com/us/en/resources/tips-articles/internet-gambling-among-teens-and-college-students>
43. L. Bojic, “Metaverse through the prism of power and addiction: what will happen when the virtual world becomes more attractive than reality?,” *Eur. J. Futures Res.*, vol. 10, no. 1, 2022.
44. S. S. Usmani, M. Sharath, and M. Mehendale, “Future of mental health in the metaverse,” *Gen. Psychiatr.*, vol. 35, no. 4, p. e100825, 2022.
45. R. Lillibridge, 2022. “Socializing in the metaverse - science, translated,” *Science, Translated - Science*.
46. N. J. Patel, “Reality or fiction?,” *Kabuni*, 21-Dec-2021. [Online]. Available: <https://medium.com/kabuni/fiction-vs-non-fiction-98aa0098f3b0>
47. K. Singh, “There’s not much we can legally do about sexual assault in the metaverse,” *Refinery29*, 09-Jun-2022. [Online]. Available: <https://www.refinery29.com/en-us/2022/06/11004248/is-metaverse-sexual-assault-illegal>
48. C. Eberhart, “Metaverse experts reveal if you can MURDER someone in virtual world – and whether you can be punished if y,” *The US Sun*, 10-Apr-2022. [Online]. Available: <https://www.the-sun.com/tech/5066296/can-you-murder-in-metaverse>
49. Ciaran Daly, “Metaverse murders could be punished just like real crimes under tough new rules,” *Dailystar.co.uk*, 01-Jun-2022. [Online]. Available: <https://www.dailystar.co.uk/tech/news/murders-metaverse-could-punished-just-27120692>
50. A. Crawford and T. Smith, “Metaverse app allows kids into virtual strip clubs,” *BBC*, *BBC News*, 23-Feb-2022.
51. R. Hu, “Understanding children’s vulnerabilities in the metaverse: the role of the online community,” *Parenting for a Digital Future*, 15-Jun-2022. [Online]. Available: <https://blogs.lse.ac.uk/parenting4digitalfuture/2022/06/15/metaverse-vrchat>
52. B. Falchuk, S. Loeb and R. Neff, “The Social Metaverse: Battle for Privacy,” in *IEEE Technology and Society Magazine*, vol. 37, no. 2, pp. 52-61, June 2018, doi: 10.1109/MTS.2018.2826060.
53. A. Bosworth, F. R. Labs, N. Clegg, and Global Affairs, “Building the metaverse responsibly,” *Meta*, 27-Sep-2021. [Online]. Available: <https://about.fb.com/news/2021/09/building-the-metaverse-responsibly>
54. L. B. Rosenberg, “The growing need for metaverse regulation,” in *Lecture Notes in Networks and Systems*, Cham: Springer International Publishing, 2023, pp. 540–547.
55. C. B. Fernandez and P. Hui, “Life, the Metaverse and Everything: An Overview of Privacy, Ethics, and Governance in Metaverse,” 2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW), Bologna, Italy, 2022, pp. 272-277, doi: 10.1109/ICDCSW56584.2022.00058
56. “Protecting children in the metaverse: it’s easy to blame big tech, but we all have a role to play,” *Lse.ac.uk*. [Online]. Available:

- <http://eprints.lse.ac.uk/114781/1/parenting4digitalfuture-2022-03-23.pdf>. [Accessed: 19-Jun-2023].
57. NIST. [Online]. National Institute of Standards and Technology (NIST): Cybersecurity Framework. Available: <https://www.nist.gov/itl/smallbusinesscyber/planning-guides/nist-cybersecurity-framework>.
  58. E. Stavrou, "Back to basics: Towards building societal resilience against a cyber pandemic," *J. Syst. Cybern. Inf.*, vol. 18, no. 7, pp. 73–80, 2020.
  59. W. J. Triplett, "Addressing Cybersecurity Challenges in Education," *ijses*, vol. 3, no. 1, pp. 47–67, 2023.
  60. C. Moumouh, M. Y. Chkouri, and J. L. Fernández-Alemán, "Cybersecurity awareness through serious games: A systematic literature review," in *Lecture Notes on Data Engineering and Communications Technologies*, Cham: Springer International Publishing, 2023, pp. 190–199.
  61. M. M. Inceoglu and B. Cilogluligil, "Use of Metaverse in Education," in *Computational Science and Its Applications – ICCSA 2022 Workshops*, Cham: Springer International Publishing, 2022, pp. 171–184.
  62. Globalauthorid. "Adaptive serious games to teach cybersecurity concepts using a machine learning approach" [Online]. Available: <http://www.globalauthorid.com/>
  63. M. Hofmeier and U. Lechner, "Operation digital ant: A serious game approach to collect insider threat scenarios and raise awareness," in *European Interdisciplinary Cybersecurity Conference*, 2021.
  64. M. Leitner et al., "AIT cyber range: Flexible cyber security environment for exercises, training and research," in *Proceedings of the European Interdisciplinary Cybersecurity Conference*, 2020.
  65. K. Heid, J. Heider, and K. Qasempour, "Raising security awareness on mobile systems through gamification," in *Proceedings of the European Interdisciplinary Cybersecurity Conference*, 2020.
  66. D. F. Povse, "It's all fun and games, and some legalese: Data protection implications for increasing cyber-skills of employees through games," in *Proceedings of the Central European Cybersecurity Conference 2018*, 2018.
  67. M. Khader, M. Karam, and H. Fares, "Cybersecurity Awareness Framework for academia," *Information (Basel)*, vol. 12, no. 10, p. 417, 2021.
  68. Center for Cybersecurity and Cyber Operations. Available online: <https://nps.edu/web/c3o/cyberciege>
  69. R. Röpke, R., U. Schroeder. The Problem with Teaching Defence Against the Dark Arts: A Review of Game-based Learning Applications and Serious Games for Cyber Security Education. In *Proceedings of the 11th International Conference on Computer Supported Education*, Heraklion, Greece, 2–4 May 2019.
  70. C. Mio, E. Ventura-Medina, and E. João, "Scenario-based eLearning to promote active learning in large cohorts: Students' perspective," *Comput. Appl. Eng. Educ.*, vol. 27, no. 4, pp. 894–909, 2019.
  71. CISA. 2022. Cybersecurity & Infrastructure Security Agency: Cybersecurity Games. [Online]. Available From: <https://www.cisa.gov/cybergames/>