Contemporary Readings in Law and Social Justice
ISSN: 1948-9137, e-ISSN: 2162-2752
Vol 17 (01), 2025
pp. 1153 – 1169

The Metaverse: An Emerging Environment for AI-Powered Crimes – Social Engineering as a Case Study

Dr. Samia Benadid[1]*

[1]Faculty of law and political sciences, University of SOUK AHRAS ALGERIA, Algeria.

Email: samia.benadid@univ-soukahras.dz

Abstract

The metaverse is an internet-based virtual three-dimensional environment where registered users who have created an avatar can actually enter with full consciousness, feeling, awareness, perception, and emotions into a multidimensional environment. They have a life in this environment that exists differently from their real life. At the same time, they can enjoy and suffer, feel different pleasures, converse, and enjoy and experience pleasure and satisfaction for their senses and emotions. fairly realistic life experiences.

the metaverse is more than a place for gaming and fun; it is an arena where people can use blockchain technology and large-scale virtual world technologies to participate in activities such as: Virtual assets and digital currency help make a nation a destination of choice for business and investment. It has become more appealing to hackers and thieves who use it to participate in things that would be painful and are prohibited in the real world.

Social engineering crimes depend only on the temptation and ambiguity of the metaverse as well as on the effectiveness of social engineering methods in constructing untrue narratives. keeping in mind the deficiencies of current juridical systems in regulating these digital worlds and the ineffectiveness of conventional artificial intelligence protection strategies in offering users privacy protection.

Keywords: Metaverse, Avatar, Social Engineering, Privacy, Cybersecurity, Deception, Victims.

Received: 12/05/2025 **Accepted:** 26/09/2025 **Published:** 16/11/2025

Introduction:

The rise of metaverse platforms has led people to engage in deep psychological and mental immersion, to the point of naively and voluntarily disclosing personal information and hidden secrets in an attempt to connect socially and build psychological bonds with virtual friends. This is part of an effort to break free from the conventional ways of building human relationships in the physical social reality.

However, alongside these naïve participants, there is another group of users characterized by intelligence, skill, and mental capacity to plan, control, and influence the audience, breaking down psychological and mental defense barriers such as doubt, caution, and hesitation. This enables them to effortlessly violate others' private lives, and their capabilities are enhanced when they apply social engineering methods and tools in the immersive environment of the metaverse.

Importance of the Study:

In order to understand the extent to which social engineering in the metaverse is being manipulated to commit an unprecedented range of crimes on the money of the victims, their personal lives, and on computer security, this research starts. A quantum leap in cybercrime in the direction of merging the metaverse with social engineering warrants research, investigation, and study to discover its scope and the tools and tactics to use for such crimes.

Problem Statement:

Driven and transformed by AI technology, the metaverse creates new frontiers of human interaction to the deployment of social engineering using human vulnerabilities. The action obliterates the lines of suspicion and suspicion the human mind uses as defenses against any suspicious act to violate one's personal space. Metaverse unity with social engineering is a new form of cybercrime that needs proper research and study to establish its tools. criminal behavior patterns and the victim's role in the facilitation of the cybercrime. This prompts us to question: What is the metaverse, and how does it combine with the dark side of social engineering? What are the new offenses that are taking shape as a result of this combination?

Methodology:

This research looks at social engineering strategies as well as the metaverse as a technology that has developed into an immersive virtual life model using a descriptive and analytical method. By looking at how they have grown to be a fixation outside of the scope of reason, this method tries to grasp the reality and the philosophy underpinning both phenomena. It will also clarify their relationship and how they influence the development of cybercrime activity.

Study Scheme:

We have broken down the plan as follows to investigate this subject:

• **Chapter 1**: The metaverse's nature together with social engineering, the technologies and techniques employed in each.

• **Chapter 2**: Social engineering, the metaverse, and their combined criminal use.

Chapter 1: Technologies and tools employed in each of the nature of the metaverse and social engineering as well as

Taking advantage of the flaws of conventional social media channels, the metaverse was created employing extremely sophisticated technology depending on several artificial intelligence technologies. It is fueled by the wishes of people who are passionate about experiencing amazing experiences in the virtual world so they may feel empowered, independent, and private. This is either by getting experiences more satisfying to their hobbies or interests, independent of self-censorship or societal norms, or because of the apparent secrecy and privacy it offers.

Social engineering strategies have grown and flourish in this atmosphere. Along with its flaws, the power, popularity, and appeal of the metaverse give a perfect backdrop for risky and bad actions that snare gullible consumers looking for many kinds of fulfillment. In this chapter, therefore, we will first examine: The Metaverse's Concept and Development (Section 1), then Social Engineering Strategies on Metaverse Platforms (Section 2).

Section 1: The Metaverse's Idea and Development

The metaverse is a three-dimensional virtual world where people who have signed up on the platform and made a virtual identity, called an "avatar," can With awareness, perception, senses, and emotions, they dive whole-heartedly into a multi-dimensional world. In this world, they lead a rich experience entirely independent from their actual circumstances. They delight in several pleasures, have talks, feel happiness and grief, and find satisfaction and fulfillment of their emotions and senses. They to some degree have actual experiences.

Subsection 1: Understanding the Metaverse

Artificial intelligence is the most recent invention in technology supported by the metaverse. Since this technology is still in its infancy and shrouded in mystery, it is a notion of ambiguity[1].

Two words—meta, which means "beyond" or "after," and verse, which means "world" or "universe"[2]—give the word metaverse its origin. Together, they create the phrases "beyond the world" or "multiverses," which are sometimes known as enhanced or parallel virtual reality. It is a place beyond reality where virtual environments and the physical world are linked together in a network. Continuous, multi-person interactions

[1] Eu blokchan,observatory and forum, Trend Report of virtual wrlds(metaverse) vertul worlds and the EC communication on virtual worlds and web 4.0(july2023),p1.
- what is the metaverse,www.newamerica.org, 04/10/2025 ,h 12:58 pm ,p2.

[2] Warda Ghriman Al-Omari, The Metaverse: Its Concept, Features, Drawbacks, and Potential Benefits in Education, A New Learning Platform, Creative Commons License, November 10, 2023, Link.
Rami Metwally Al-Qadi, Forensic Guide in Metaverse Technology, Arab Journal of Security Studies, Naif Arab University for Security Sciences, Saudi Arabia, Volume 39, Issue 2, p. 192. Singh J., Singh P. ,Kaur r,K a, Hedabou m, privacy and security in the metaverse :trends ,challengs,and future directions ,IEEE Access mulidixiplinary,vol 13,2025, p12021.

abound in the metaverse, where symbolic avatars depict users. These avatars interact in real time to give consumers an immersive experience[3].

Subsection 2: The Development of the Metaverse and the Tools Found in It

The metaverse is a multi-vendor, large cloud-distributed social network accessible on several linked devices. This idea combines Web 2.0 and Web 3.0 techniques to give the existing internet an interactive overlay. Relying on artificial intelligence (AI), it combines Virtual Reality (VR), Augmented Reality (AR), Mixed Reality (MR), and 3D environments (D3). Offering a genuine immersion of the user into a virtual reality world simulating the real world, the engagement in the metaverse is real-time, efficient, and ongoing[4]. It lets people buy and sell, play games, and talk to each other through chat, among other things[5].

The word "metaverse" originally showed up in Neal Stephenson's 1992 book Snow Crash, created by the author. Additionally, it saw utilisation on virtual world systems like Second Life. Authors at DC Comics started calling a core version of reality that shapes other versions in alternate timelines the "metaverse" in 2019[6].

The word has since come to refer to an idea of future iterations of the internet made up of distributed, always-connected, 3D simulations[7]. With Second Life (introduced in 2003), the first metaverse to feature avatars, the metaverse has produced several platforms. Facebook Meta (formerly Facebook) created Horizon Worlds, a virtual environment[8].

Subsection 3: The Meaning of Avatar Symbols

Two-dimensional emojis inspire avatars, who stand for people in virtual settings like the metaverse worlds. Users can engage, travel, and explore the platform using avatars in a manner quite like human interaction. Originally, avatars featured movie or game characters, cartoon characters, or emojis. But as technology progressed, avatars were made with AI techniques to look like humans, which made them look more real by using generative AI and deepfake methods.

For participants in electronic games, social media sites, and educational platforms, avatars seek to offer a more genuine experience. Because they act as the interaction interface between users, avatars are quite important in the metaverse world. Apart from being a digital persona the account holder alone manages, avatars are the only way to

---

3 Mystakidis, S., "Metaverse," Encyclopedia, pp. 486-497. DOI: 10.3390/encyclopedia201031, November 10, 2023. Zaiter Nour El-Din, "The Virtual World of the Metaverse: A Psychological Perspective," Journal of Human Sciences, University of Oum El Bouaghi, Algeria, Volume 09, Issue 02, June 2022, pp. 1018, 1020.

4 Muadh Suleiman Al-Mulla, "Metaverse Technology – New Challenges in Criminal Law: A Descriptive Analytical Study," *Journal of the Kuwait International Law College*, 11th Year – Special Supplement – Issue 14, Safar 1445 AH, September 2023, p. 8.Islam Mustafa Gomaa Mustafa, "Crimes Committed Using Modern Technology in Egyptian Law (Virtual Reality, Augmented Reality, and Mixed Reality)," *D M*, Issue 38, First Edition, 2022, pp. 7, 8.

5 Kashif Laeeq, "Metaverse: Why, How, and What," ResearchGate, Visit Date: November 11, 2023.

6 "Doomsday Clock Just Redefined the Entire Multiverse," CBR, May 29, 2019.

7 Casey Newton, "Facebook CEO on Why the Social Network is Becoming 'A Metaverse Company,'" *The Verge*, July 22, 2021, 3 PM, Visit Date: November 10, 2023.

8 Warda Ghriman Al-Omari, *Op. Cit.*, No page number.

engage in and immerse oneself in the virtual world[9]. They let consumers manage email accounts, arrange meetings, produce reports, interact, finish everyday tasks, improve efficiency and productivity, and do virtual chores including interacting.

Subsection 2: Social Engineering Techniques on Metaverse Platforms

Social engineering is the essence of virtual worlds, including the metaverse, as it is fundamentally the reason for the creation of these worlds. The overwhelming feelings and emotions, swinging between desire, curiosity, trust, hesitation, and susceptibility to pressure, are what drive people to immerse themselves in these environments to experience the highest levels of human inclination, free from the constraints of conscience, law, and ethics at times.

However, in the pursuit of adventure through creating a series of semi-real relationships in what is believed to be a private world, a person creates a parallel universe to their real life in which they are freed from all life's constraints. They then fall victim to negative social engineering, becoming prey to a solitary fraudster or a criminal group that exploits the strengths of social engineering and the metaverse platforms, as well as the victims' psychological weaknesses. These perpetrators manipulate victims to extract sensitive information or gain unauthorized access to digital assets, databases of digital entities, and more.

We will first discuss the **definition of social engineering** (Subsection 1), followed by **AI tools supporting social engineering techniques** (Subsection 2).

Subsection 1: Definition of Social Engineering

Social engineering, at its core, is a science that studies efforts to influence public opinion and social behavior on a wide scale, either by governments or private groups that pursue special interests. It aims to manage resources on a broad scale, relying on a scientific method to study social interest using scientific methods to analyze and understand social systems in order to make decisions based on scientific, not political, considerations. This concept parallels political engineering in the field of political science.

Ferdinand Tönnies[10] defined it as a scientific system based on gathering conclusions and technical decisions that include reliable statistical data, which can be applied to the social system to create a sustainable design for intelligent management.

Christopher Hadnagy defined social engineering as "a set of patterns and behaviors that are deliberately practiced, usually legally, in marketing to persuade a targeted consumer about a specific product and promote institutions. It is also used in political science to gain voter support and has other applications in education and medicine."[11]

---

[9] Manal Al-Balqasi, "Virtual Digital Characters (Avatars)," Dar Misr for Publishing and Distribution, Egypt, August 2024, pp. 157, 165.

[10] **Ferdinand Tönnies**, founder of modern sociology in Germany, with studies on community and society.

[11] **"What is Social Engineering? Methods and How to Avoid It"**, available at https://www.it-pillars.com, visited on 10/06/2023, cited in **Mohammed Dahmani**, "Cybersecurity Threats – Social Engineering as a Case Study," *Academic Journal of Legal and Political Research*, Volume 9, Issue 2, 2023, p. 291.

Unfortunately, the positive concept of social engineering quickly gained a negative connotation due to its use in committing security breaches and various crimes, especially after the spread of the internet, social media platforms, and virtual environments, including the metaverse. As a result, social engineering has become synonymous with fraud, manipulating the deep psychological concerns and desires of humans[12].

Negative social engineering, therefore, is a hacking technique that relies on manipulating the individual's mind and emotions, exploiting human error caused by carefully crafted tricks[13]. These tricks make the victim trust the fraudster due to emotional inclination, psychological obsession, fear of harm, or the desire to gain moral or material benefits. This technique is used to extract financial or material gains through gaining authorized access to confidential information. It closely resembles fraudulent maneuvers in scam crimes[14], but it relies on information technology as a means to execute the plot and occurs only in virtual environments, not in the physical world.

Subsection 2: Artificial Intelligence Tools Supporting Social Engineering Techniques

Whether in 2D or 3D virtual spaces like the metaverse, social engineering calls for the control and use of a number of artificial intelligence technologies. to create realistic almost lifelike misleading internet material. This is known as "virtual realism," and it makes the victim stop thinking critically and instead freely ignore their logical concerns and believe in false information. It more exactly reflects their attitudes and feelings[15]. AI technologies greatly improve internet fraud and magnify it in the immersive world of the metaverse, where the victim is completely absorbed in embracing the dishonest story.

Artificial intelligence (AI) is a field of computer science that aims to let computers do things that are similar to how humans think, like learning, thinking, and making decisions[16]. Artificial intelligence (AI) basically replicates human behavior in order to produce specific outcomes by independently deciding things. It does, however, depend on

---

[12] **Ziyoush Said**, "Breach via Social Engineering and Protection Methods," *Family and Society Journal*, Volume 9, Issue 2, 2021, pp. 178, 177.

[13] **Ziyoush Said**, *Op. Cit.*, p. 174. **Ihab Anan**, "Cybersecurity – Social Engineering: The Soft Weapon of Cyber Wars," *European Center for Studies on Counter-Terrorism*, Germany, ECCI, July 2024, https://x.com/ehab2anan.

[14] **A'id Raja Al-Khalayleh**, *Electronic Delictual Liability: Liability Arising from the Misuse of Computers and the Internet*, Dar Al-Thaqafa, Amman, Jordan, 2009, p. 135. **Karim Ma'arouf**, "Damages Arising from Criminal Risks in Cybercrimes," *Journal of Strategic Studies for Disasters and Opportunity Management*, Democratic Arab Center, Berlin, Issue 4, Volume 14, June 2022, pp. 93, 94. **Ben Adid Samia**, *Legal Protection for Electronic Payment Systems*, Doctoral Thesis, 2022, Faculty of Law, University of Badji Mokhtar, Annaba, p. 286.

[15] **Abdulilah Saeed Al-Mihya & Arwa Ahmed Makin**, "The Impact of Social Engineering on Cybersecurity Risks in Banks in Riyadh, Saudi Arabia," *Journal of Economics, Administrative and Legal Sciences*, Volume 9, Issue 1, 2025, Link, p. 4.

[16] **Asmaa Belita**, "Legal and Regulatory Codification of Artificial Intelligence in Algeria," *International Journal of Artificial Intelligence in Education and Training*, University of Algiers (1), January 2022, p. 19. **Ghofran Mohamed Ibrahim Helal et al.**, "Governance of Artificial Intelligence within International Human Rights Law." **Journal of Studies in Sharia and Law Sciences**, Volume 49, Issue 4, 2022, University of Jordan, pp. 126-138. DOI: 10.35516/law.v49i4.173, site visited on 12/11/2023.

algorithms with inputs. outputs that can only be used with physical material means. The most important AI tools are:

First: Data Mining Techniques

Data mining refers to a set of computer techniques designed to automatically mine large volumes of integrated data to identify unexpected or hidden patterns or information. It is also known as knowledge discovery in databases[17]. During the data mining process, data is analyzed, linked, compiled, counted, and classified to extract useful insights, which are then employed in decision-making processes. These are referred to as predictive hidden insights. The main goal of data mining is to maintain data quality. Predictive data mining is widely used in commercial businesses, while descriptive mining is essential in the stages of data exploration, such as aggregation, statistics, and summarization[18].

Second: Generative Artificial Intelligence (AI)[19]

Generative AI is a form of artificial intelligence that can create text, images, and diverse content based on the data it is trained on. It generates new content in any format because it learns from the data it accesses and creates new data copies that are not necessarily real[20]. Generative AI learns from data rather than explicit programming because it has the ability to adapt to new data independently, using machine learning techniques. It can be conversational AI, which understands and responds to human language. There are two types of generative AI: one is used for data analysis and generating text or images, and the other is interactive AI, which participates in conversations as if it were human. Thus, generative AI includes both conversational and interactive forms[21].

Third: Deep Fake Technology

Deep fake is a technology that creates fake images and videos using computer programs based on machine learning and AI techniques. It combines several images or video clips of a person to generate a new clip that appears real at first glance. The *video rewrite* program, released in 1997, was the first of its kind[22]. The term "deep fake" emerged in late 2017 from a Reddit user who called themselves "deepfakes." In 2018, Reddit banned the use of deep fake technology due to its malicious use.

---

[17] **Anwar Fadil Al-Farsi**, "The Role of Data Mining Techniques as One of the Information Technology Innovations in Improving the Quality of Financial Reports: A Field Study," *Scientific Journal of Financial and Administrative Studies and Research*, Volume 13, Issue 02, March 2022, pp. 641-642.

[18] **Anwar Fadil Al-Farsi**, *Op. Cit.*, p. 644.

[19] **Imad Abdul Rahim Al-Duhyat**, "Towards a Legal Regulation of Artificial Intelligence in Our Lives – The Issue of the Relationship Between Humans and Machines," *Journal of Judicial Ijtihad for Legal and Judicial Studies*, Volume 08, Issue 05, 2019, p. 16.

[20] **Rasha Mustafa Awad**, "Industry and Combat: How Artificial Intelligence Is Changing the Economic Crime Landscape," *Special Studies*, Future Foundation for Research and Advanced Studies, Abu Dhabi, UAE, Issue 29, July 2024, p. 08.

[21] **Ghofran Mohamed Ibrahim Helal et al.**, *Op. Cit.*, p. 126.

[22] - Covell Michele, Bregler christoph, Cloney Malcom, 1997 « video rewrite, Driving visual speech with audio», Droceedings of the 24th Annule conference on computer graphics and interactive techniques, ACM, Digital library, 19.05.2020,pp 353-360.

The Fake App software for computers came out in January 2018. It made it easy for people to make and share videos by switching faces. It makes use of graphic processors and artificial neural networks. Deep Face and Face Swap are two open-source programs that can be used instead of Fake App[23].

Fourth: Synthetic Data Fabrication (SDF)

Synthetic data generation (SDF)[24] uses techniques to fabricate or alter data with the aim of deceiving persons or organizations. This is achieved by generating false identities through the mixture of real information and false data, which is then used in scams. It is an advanced method that cannot be detected since no identity theft occurs, and consequently, it is not reported. This technique is a highly advanced form of conducting numerous illegalities, the most notable of which is phishing attacks[25]. They have victims ranging from individuals to banks and financial institutions[26], which are subject to actual world threats from this technique.

Subsection 3: Designing a Fraudulent Scheme Using Social Engineering Techniques

Social engineering has several techniques that can be used to deceive the victim. The first technique that can be used is by deceiving the victim using a tempting information package, whereby fake CDs, messages, or websites are left for the victim to respond to without any interaction from the fraudster. This type of social engineering is called negative social engineering[27]. The second type, and also the commonly used technique in the metaverse, is called positive social engineering, whereby communication takes place from the fraudster, using his or her avatar, to the victim.

In both situations, the fraudster carries out a carefully designed fraudulent plan in several stages, as follows:

- **Targeting the victim[28]**: The first step is identifying the victim by determining the personality traits that the fraudster will focus on in crafting their fraudulent scheme. The victim's patterns vary according to the fraudster's inclinations and the intended objectives, such as targeting minors for producing explicit digital content or blackmail, or targeting women in special social situations such as widows, divorcees, or single women, or choosing a victim based on their financial status or job position.
- **Gathering information**: This is done using **data mining techniques**, analyzing, linking, compiling, and classifying data to extract useful insights. These insights are then used to assist in decision-making processes.

---

[23] **"Deep Face"**, a tool that utilizes machine learning to replace faces in videos, includes pre-built, ready-to-use standalone binary files for Windows 7, 8, and 10. — Iperov DF, 09.05.2019.

[24] **Ben Ouda Askar Murad**, "The Issue of Applying Criminal Liability Provisions to Artificial Intelligence Crimes," *Journal of Law and Human Sciences*, Volume 15, Issue 01, 2022, p. 192.

[25] **Sami Mohamed Bouneff**, "The Role of Proactive Strategies in Facing Cyberattacks: Cyber Deterrence as a Case Study," *Algerian Journal of Law and Political Sciences*, University Center "El-Wenchesris," Tissemsilt, Algeria, Volume 04, Issue 07, June 2019, p. 125.

[26] **Ahmed F. Moussa, M. Hasna, Z. Jaffal, J. Barafi**, "Artificial Intelligence Crimes," *Academic Journal of Interdisciplinary Studies*, www.richtmann.org, January 2023, p. 145.

[27] **Abdulilah Saeed Al-Mihya & Arwa Ahmed Makin**, *Op. Cit.*, p. 4.

[28] **Said Ziyoush**, *Op. Cit.*, p. 175. Likewise, **Mohammed Dahmani**, *Op. Cit.*, p. 695.

- **Designing the narrative or fake identity**: The next step is to create a fake backstory or identity, which is used to establish contact with the victim and initiate direct interaction. This process utilizes **generative AI techniques**, **deepfake technology**, and **synthetic data fabrication**, which is part of orchestrating the fraudulent maneuver.
- **Starting the interaction and building trust**: Initiating interaction with the victim and gaining their trust is the pinnacle of the design behind social engineering. The ultimate goal from the beginning is to establish this interaction and earn their trust, pushing the victim to disclose confidential or legally protected information or information that is not available under contractual obligations.

In the metaverse platform, the process of gaining trust and starting interaction via the avatar goes beyond simple virtual technical interaction, as seen in other social media or 2D websites. The communication is sensory because the victim is connected to their avatar or virtual symbol using a digital headset and sensory devices that send neural messages to the brain, causing the person to react psychologically and sensorially as if they were in the physical world.

This makes it difficult for the victim to verify the credibility of the signals they receive from the fraudster[29], as they are immersed in an environment that gives them a false sense of security, facilitated by AI tools that make the interaction extremely realistic[30]. The avatar can simulate interactions, gestures, and cues flawlessly due to the use of machine learning algorithms that analyze user behavior, preferences, and weaknesses.

•Implementation/acquisition stage, followed by disconnection and disappearance:[31] This is where the fraudster, having established a connection with the victim, carries out the fraud action, mainly by convincing the victim to release crucial information that ought not to be shared, or making it possible for the fraudster to access the information or procuring it for themselves. This could also include convincing the victim to perform several tasks, for example, making financial payments, blackmail, and so forth. The victim, either through blindly trusting the fraudster, fearing harm to themselves, or through intimidation to expose something that could embarrass them or their family, complies with the fraudster's request and releases the entrusted information.

Once the fraudster has obtained the information or carried out financial transactions, they cut every connection with the victim, remove any digital trails, and disappear, knowing that the account began as a fraud.

Chapter 2: The Metaverse and Social Engineering: Mutual Criminal Exploitation

The fixation on modern technology and the unending quest for the latest innovations from the technological world has become the defining attribute of the 21st century. With each new release of an update, application, or platform, the 'enthusiasts and addicts' continuously reach ever-increasing heights of amazement, absorption, and immersion, at the same time casting aside reality and the disciplines, prudence, and artificial constraints imposed by reality that came along with it. The addicts become dazed, distracted, and

[29] **Manal Al-Balqasi**, *Op. Cit.*, p. 165.
[30] **Abdulilah Saeed Al-Mihya & Arwa Ahmed Makin**, *Op. Cit.*, p. 4.
[31] **Mohammed Dahmani**, *Op. Cit.*, p. 696.

unsuspecting, prey to manipulation and deceit. This comes through their loss of discretion and unlimited credulity, leading to the loss of their guise of anonymity, making them 'victims of their own making.' This can be observed in their 'activities in the virtual world,' proving to be 'malleable instruments' for 'serious cybercrimes.' This issue will be discussed in the 'following sections' that will illustrate: Security Breatches in Metaverse Platforms (Section 1), Risks of Criminal Social Engineering (Section 2).

Section 1: Security Breaches in Metaverse Platforms

The metaverse sets the stage for social engineering attacks like never before. Here, scammers hide behind virtual avatars, take advantage of weak security, and slip through the cracks left by inconsistent rules across platforms. Advanced AI tools power this digital world, but instead of solving old problems, they crank them up. The metaverse doesn't escape the flaws of the real world—it ends up making them worse. In this section, we'll look at how social engineering thrives in the metaverse and what kinds of security breaches follow.

Digital Identity Theft and Privacy Invasion Risks (Subsection 1), **Financial Fraud and Attacks on Virtual Assets** (Subsection 2), **Ineffectiveness of Traditional Cybersecurity** (Subsection 3).

Subsection 1: Digital Identity Theft and Privacy Invasion Risks

In the metaverse, you start by registering on a website, making your account, and building your avatar—a virtual version of you or your business. They're not cartoon cutouts anymore. Now, they're highly developed 3D or even 4D replicas that can walk and react like a human being. Through your avatar, you communicate with other individuals, either you are gaming, working, or participating in a virtual conference[32]. It's your digital identity, and you're the one in control, shaping it with your interests and preferences.

Avatars have come a long way, especially with the rise of AI and sophisticated graphics[33]. Now, they can mimic facial expressions and body language so well, it's easy to forget you're not talking to a real person. The realism blurs the line between digital and human interaction.[34]

Developing these avatars is a combination of several technologies, but deepfakes are different[35]. Deepfakes can create images and sound that are almost indistinguishable from real ones. Wonderful, but of course that presents an opportunity for abuse. Deepfakes are employed to impersonate other people, like celebrities, or to create new identities and deceive users on the platform. A scammer will send a friend request, start

---

[32] **Sandia Al-Hammadi & Imad Al-Din Abdul-Hay**, "The Identity of the Digital Trader on the Metaverse Platform," *Critical Journal of Law and Political Science*, Faculty of Law, Tizi Ouzou, Volume 19, Issue 02, 2024, p. 133.

[33] **Manal Al-Balqasi**, *Op. Cit.*, p. 160.

[34] **Manal Al-Balqasi**, *Ibid.*, p. 171.

[35] **Alaa Al-Din Mansour Mughayrah**, "Artificial Intelligence Crimes and Ways to Confront Them: Deepfake Crimes as a Model," *International Journal of Law*, Qatar University, Volume 13, Issue 2, 2024, pp. 131–133.

talking with you, gain your trust, and then look at your page. After that, they monitor your activity or install malware to access personal information[36].

Metaverse platforms collect a lot of personal information, including biometric data and financial details, supposedly to confirm your identity for your avatar. That data doesn't just stay with the company—you're exposed to hackers using AI to break in and steal it. So, every step in the metaverse, from avatar creation to interaction, carries real security risks.

Subsection 2: Financial Fraud and Attacks on Virtual Assets

The metaverse is fertile territory for electronic financial fraud[37] as one can quickly set up commercial communities on such platforms[38]. With the presence of such virtual assets as non-fungible tokens (NFTs) and virtual currency, and most countries using these assets, there have been platforms that officially govern their operations due to the profitability of such sites in transactions as well as how fast the profits are. This has made such websites highly susceptible to cybercriminals, who use such forms of scams to scam victims[39] and withdraw their money.

Subsection 3: Failure of Conventional Cybersecurity

Cybersecurity has come up as the pillar of the new era, with goals to ensure data integrity, preserve confidentiality and privacy of information, ensure smooth digital services, prevent fraud and intrusions, and protect devices and software. Yet, in the metaverse era, cybersecurity also has pressing issues in the safeguard of digital identities[40] and privacy and network security because the nature of the metaverse is unascertainable and there are no clear lines between the real and virtual worlds. The use of avatars also complicates the identification of security loopholes because it is getting harder to identify digital invasions in such immersive environments.

A future-proof or green model for cybersecurity for metaverse platforms requires an integrated approach, incorporating technological, operational as well as human aspects. Cybersecurity is an incredibly huge set of enabler fields like network security, application security, information security, operational security[41], disaster recovery, business continuity, and end-user training. They are interrelated and combined constitute multi-layered security mechanism.

---

[36] **Said Ziyoush**, *Op. Cit.*, p. 175.

[37] **Ben Adid Samia**, "Financial Fraud Using AI Tools in the Metaverse Environment," paper presented at the International Conference titled "Business Crimes in the Digital Environment," held on April 12, 2025, Faculty of Law and Political Science, University of Souk Ahras, pp. 10–11.

[38] **EU Blockchain, Observatory and Forum**, "Trend Report of Virtual Worlds (Metaverse): Virtual Worlds and the EC Communication on Virtual Worlds and Web 4.0 (July 2023)," p. 4.

[39] **Rami Metwally Al-Qadi**, "Digital Guide in Metaverse Technology," *Arab Journal of Security Studies*, Naif Arab University for Security Sciences, Volume 39, Issue 2, p. 195.

[40] **Singh J., Singh P., Kaur R., K.A., Hedabou M.**, "Privacy and Security in the Metaverse: Trends, Challenges, and Future Directions," *IEEE Access Multidisciplinary*, Vol. 13, 2025, p. 12021.

[41] **Osama Azmi Salam et al.**, "Risk and Insurance," Dar Al-Hamed, Jordan, 2007, p. 22.

Deploying a comprehensive cybersecurity strategy is more than a compliance. It needs tocover all the facets of digital infrastructure, including applications and networks down to operations and data, with specific focus on endpoint security and disaster restoration[42].

Furthermore, continued investment in new-age technologies such as AI, machine learning-based anti-fraud tools, blockchain-based transactional transparency and quantum-resistant technology for long-term security and engineering trust to restrict the risk of unauthorized access are important to reduce the metaverse platform cyberattack risk likelihood.

Subsection 2: Risks of Criminal Social Engineering

The metaverse is a tremendous step forward in technological innovation in the second decade of the new millennium. It comes with some new risks and warnings, though, because of its newness, uncertainty, and failure on the part of current laws written to counter cybercrime to handle this technology. This is owing to its fast pace of change and the specific tools and pieces of software employed within it. The metaverse is a virtual world where time and place[43] do not count, but is a theoretical space. This has been behind the creation of super-fast cybercrimes that have widened a gap between law and technology, a gap the law is struggling to close and contain to protect citizens from its risks. Here are some of them, as follows: Exploitation of Human Weaknesses (Subsection 1), Loss of Trust and Social Discrimination (Subsection 2).

Subsection 1: Exploitation of Human Weaknesses

Social engineering exploits various human weaknesses to obtain sensitive and confidential information[44] or to get the victim to do something that profits the scammer. This exploitation may take the kind of threatening to reveal a secret, making promises of easy money, or taking advantage of emotional desires, such as the desire of the victim for emotional or sexual satisfaction. Other times, the scammer exploits the victim based on their age or their mental capacity[45] to get them to undertake criminal acts.

In attempting to do so, scammers might use a variety of artificial intelligence (AI) techniques to victimize their targets, techniques that have already been mentioned earlier.

Social engineering's danger in the metaverse is its interactive, immersive, and engaging quality, which is highly convincing. The metaverse's virtual reality, with the help of

---

[42] **Fahd Fayez Al-Mudrah**, "Global Standards for Information Security," Center of Excellence for Information Security (COEIA), DSN, p. 2.

[43] **Mohammed Jibril Ibrahim Hassan**, "The Legal Framework of Metaverse Technology: A Foundational and Prospective Study," *Journal of Legal and Economic Research*, University of Mansoura, Volume 13, Issue 85, September 2023, p. [not specified].

[44] **Said Ziyoush**, *Op. Cit.*, p. 182.

[45] **Muadh Suleiman Al-Mulla**, "Metaverse Technology: New Challenges in Criminal Law, A Descriptive and Analytical Study," *Journal of the Kuwait International Law College*, 11th Year, Special Supplement, September 2023, Issue 14, pp. 14–15.

deepfake technology and other AI tools[46], distorts reality and conditions the victim for psychological manipulation. This leads the victim to blindly trust the scammer, propelled by a condition of being overpowered by emotions that render their defense mechanisms ineffective, such as skepticism, hesitation, and logical thinking[47]. This state of confusion leaves the victim confusing the virtual reality with an existing and trustworthy platform.

Subsection 2: Loss of Trust and Social Discrimination

The use of virtual avatars as digital identities while navigating the metaverse platforms is a challenge in reality. The function of the avatar goes beyond being a means of digital identification; in some perspectives, it is also considered part of the user's personal data. As such, it needs to be under the same legal safeguard when it comes to personal data[48].

Also, the user can use the avatar as a mask to commit crimes that harm others' reputation and honor. Avatars are also used for bullying, hate speech, racism, exclusion, marginalization, and ethnic or religious discrimination[49].

Similar to social media, the metaverse has the extraordinary ability to impact public opinion[50] and attract followers using deepfake technology and social engineering. It distorts the authenticity of public opinion polls and surveys, generating a virtual public opinion that does not exist in reality.

As a result of this, a decrease has been observed in the faith in the credibility of information and analysis released in the conventional or digital media, especially with regard to the content released on virtual platforms. Social discrimination, as well as cultural, racial, and ethnic discrimination, has also been witnessed again after the spread of hate speech and incitement, both explicit and implicit, through virtual gaming platforms.

Conclusion

The development of modern technologies using artificial intelligence has led to the emergence of a new mode of human interaction after social media, namely the metaverse, which primarily relies on AI tools, especially social engineering.

This has resulted in a new form of cybercrime, unlike anything seen before, in terms of its methods, tools, and victims. The allure and brilliance of the metaverse, with its captivating and diverse worlds, has absorbed participants and overshadowed their lives. Its enchantment has dulled their awareness, breaking down the walls of intuitive defense or instinctual caution, causing them to voluntarily abandon their defenses and allow their

---

[46] **Siva K. J.**, "Social Engineering 2.0: Deepfake and Deep Learning-Based Cyberattacks (Phishing)," *International Journal for Multidisciplinary Research (IJFMR)*, www.ijfmr.com, Vol. 07, Issue 1, January-February 2025, p. 7.

[47] **Abdulilah Saeed Al-Mihya et al.**, *Op. Cit.*, p. 10.

[48] **Muadh Suleiman Al-Mulla**, *Op. Cit.*, p. 22.

[49] **Haya Center for Public Policies**, "Countering Hate Speech Online," Amman, Jordan, 2015, p. 4. **Amnesty International** defined discrimination as "the imbalance in equality between individuals or its absence," 26/04/2021, 23:44, Link.

[50] **Muadh Suleiman Al-Mulla**, *Ibid.*, p. 16.

private lives to be opened to strangers who offer them false warmth and attention at times, or threats and doubts at others. Consequently, they become victims of their desires and hand over secrets and information they should have kept confidential. They fall hostage to fraudsters who, by controlling AI tools, seize wealth, manage fake bank accounts, and threaten the lives of individuals whose only crime is their obsession and unconscious immersion in new, obscure, and poorly defined digital spaces, with the primary tool being negative social engineering, which exploits human weakness in the face of temptations and the obsessive search for virtual acceptance.

Thus, after studying the nature of both the metaverse and social engineering, it became clear that the metaverse is a new virtual environment that is legally undefined and has yet to be given a standardized definition by technical experts, let alone legal authorities. As a result, its dimensions, boundaries, and temporal and spatial scope have not yet been defined.

We also learned about social engineering and how it transformed from a science with positive dimensions, aiming to uplift humanity by understanding collective thinking patterns on issues that concern people, into a negative tool used to ensnare victims. This transformation exploits human psychological weaknesses, such as greed, emotional deprivation, fear, hope, and loneliness, turning these into weapons aimed at these victims, ultimately leading them into the traps of cunning fraudsters who control technology to achieve quick gains at the expense of people's lives, dignity, and security.

According to these observations, we have reached the following important conclusions:

••The metaverse has not yet been defined officially. All the definitions that we have are technically strict, produced by high-tech investment firms and done for business purposes, so that the definition remains loose so that the metaverse can continue to attract and flourish.
•Social engineering is an old science that has been remodeled to be used as a means of cyber intrusion, particularly in the metaverse. It does not depend on AI technology alone but also on participants' addiction and immersion in the enigmatic worlds of the metaverse, where they abandon emotional self-control and intentionally cease employing their minds, disregarding cautionary measures and critical thinking in defense of their personal space.
•The tech glitches in the metaverse, such as the absence of standard security protocols and protection policies against privacy that consider the unique nature of the metaverse—especially in protecting biometric and personal data as well as preventing it from being shared with third parties—are sufficient to raise serious concerns about participants' safety. Moreover, participants' insufficient control over programming as well as cybersecurity processes exacerbates these threats.

Given the fact that current legal frameworks, whether in conventional or cybercrime, cannot handle the new forms of crime in the metaverse, which are unique to the virtual environment, we suggest the following:

•A critical need exists for the development of a full and cohesive definition of the metaverse beyond the current narrow definitions. This will enable the establishment of a legal regime for the metaverse from all aspects, including criminal judicial jurisdiction.

•A need exists to regulate document mechanisms such as encryption, digital signatures, and legally accrediting avatars as part of the personal data to be protected by law.
•Develop an abuse and complaint mechanism for the victims of social engineering, criminalizing cheating activities, cyberbullying, and race discrimination in this case.
•Implement a uniform security policy for every metaverse platform and subject them to security levels by adding tools and technologies that allow monitoring and tracing all forms of manipulation on these platforms.

References:

1. Warda Ghrman Al-Omari, *The Metaverse: Its Concept, Features, Drawbacks, and Potential Benefits in Education*, New Learning Platform. http://creativecommons.org/licenses/by-(nc-sa)3.0.2023/11/10m
2. Rami Metwally Al-Qadi, *The Forensic Guide in Metaverse Technology*, The Arab Journal of Security Studies, Naif Arab University for Security Sciences, Saudi Arabia, Vol. 39, Issue 2.
3. Zaiter Nour Eddine, *The Virtual World of the Metaverse from a Psychological Perspective*, Journal of Human Sciences, University of Oum El Bouaghi, Algeria, Vol. 09, Issue 2, June 2022.
4. Moath Suleiman Al-Mulla, *Metaverse Technology: New Challenges in Criminal Law – A Descriptive and Analytical Study*, Kuwaiti International Law College Journal, 11th Year, Special Supplement, Issue 14, Safar 1445H, September 2023.
5. Islam Mustafa Gomaa Mustafa, *Crimes Committed Using Modern Technology in Egyptian Law (Virtual Reality, Augmented Reality, and Mixed Reality)*, M.D., Issue 38, 2022, First Edition.
6. Manal Al-Balqasi, *Virtual Digital Characters (Avatars)*, Dar Misr for Publishing and Distribution, Egypt, August 2024.
7. Mohamed Dahmani, *Cybersecurity Threats – A Case Study in Social Engineering*, The Academic Journal of Legal and Political Research, Vol. 9, Issue 2, Year 223.
8. Ziyoush Said, *Hacking through Social Engineering and Methods of Protection*, Journal of Family and Society, Vol. 9, Issue 2, 2021.
9. A'id Rajaa Al-Khalayla, *Electronic Negligence Liability: Liability Resulting from Misuse of Computers and the Internet*, Dar Al-Thaqafa, Amman, Jordan, 2009.
10. Karim Ma'ruf, *Damage Resulting from Criminal Risks in Cybercrimes*, Journal of Strategic Studies for Disasters and Opportunity Management, The Democratic Arab Center, Berlin, Issue 4, No. 14, June 2022.
11. Ben A'did Samia, *Legal Protection of Electronic Payment Systems*, PhD Thesis, 2022, Faculty of Law, Badji Mokhtar University, Annaba.
12. Abdulilah Said Al-Mohaya and Arwa Ahmed Makin, *The Impact of Social Engineering on Cybersecurity Risks in Banks in Riyadh, Saudi Arabia*, Journal of Economics, Administrative Sciences, and Law, Vol. 9, Issue 1, 2025, http://journals.ajsrp.com/index.php/jeals.
13. Asma Belaylita, *Legal and Regulatory Recognition of Artificial Intelligence in Algeria*, International Journal of Artificial Intelligence in Education and Training, University of Algiers (1), January 2022.
14. Ghufran Mohamed Ibrahim Hilal et al., *AI Governance within International Human Rights Law*, Journal of Studies, Sharia and Law Sciences, Vol. 49, Issue 4, 2022, University of Jordan, Visit Site: 12/11/2023.

15. Anwar Fadil Al-Farsi, *The Role of Data Mining as an Innovation in Information Technology to Improve the Quality of Financial Reports: A Field Study*, Scientific Journal of Financial and Administrative Studies, Vol. 13, Issue 2, March 2022.
16. Emad Abdelrahim Al-Dahiyat, *Towards Legal Regulation of Artificial Intelligence in Our Lives: The Issue of Human-Machine Relationships*, Journal of Judicial Studies for Legal and Judicial Studies, Vol. 8, Issue 5, 2019.
17. Rasha Mustafa Awad, *Industry and Combat: How Artificial Intelligence Is Changing the Landscape of Economic Crime*, Special Studies, Future Research and Advanced Studies Institute, Abu Dhabi, UAE, Issue 29, July 2024.
18. Ben Awda Askar Murad, *The Issue of Applying Criminal Liability Provisions to AI Crimes*, Journal of Law and Humanities, Vol. 15, Issue 1, 2022.
19. Sami Mohamed Bounif, *The Role of Proactive Strategies in Facing Cyberattacks: Cyber Deterrence as a Model*, Algerian Journal of Law and Political Sciences, "El Wenshris" University Center, Tissemsilt, Algeria, Vol. 4, Issue 7, June 2019.
20. Sandia Al-Hamadi and Emad El-Din Abdel Haye, *The Digital Merchant Identity in the Metaverse Platform*, Critical Journal of Law and Political Science, Faculty of Law, Tizi Ouzou, Vol. 19, Issue 02, 2024.
21. Alaa Eldin Mansour Mughayrah, *AI Crimes and Ways to Address Them: Deepfake Crimes as a Case Study*, International Journal of Law, Qatar University, Vol. 13, Issue 2, 2024.
22. Ben A'did Samia, *Financial Fraud Using AI Tools in the Metaverse*, Presentation at the International Conference on "Business Crimes in the Digital Environment," April 12, 2025, Faculty of Law and Political Sciences, University of Souk Ahras.
23. Rami Metwally Al-Qadi, *Digital Evidence in Metaverse Technology*, The Arab Journal of Security Studies, Naif Arab University for Security Sciences, Vol. 39, Issue 2.
24. Osama Azmi Salam et al., *"Risk and Insurance"*, Dar Al-Hamid, Jordan, 2007.
25. Fahd Fayez Al-Mudrah: *Global Standards for Information Security*, Center of Excellence for Information Security (COEIA), DES N.
26. Mohamed Jibril Ibrahim Hassan, *The Legal Framework for Metaverse Technology: A Foundational and Foresight Study*, Journal of Legal and Economic Research, University of Mansoura, Vol. 13, Issue 85, September 2023.
27. Haya Center for Public Policy, *Combating Hate Speech Online*, Amman, Hashemite Kingdom of Jordan, 2015.
28. Eu Blockchain, Observatory and Forum, *Trend Report of Virtual Worlds (Metaverse): Virtual Worlds and the EC Communication on Virtual Worlds and Web 4.0* (July 2023).
29. New America, *What Is the Metaverse?* www.newamerica.org, 04/10/2025, 12:58 PM.
30. Kashif Laeeq, *Metaverse: Why, How, and What*, http://www.researchgate.net/publication/35805001 (Visited: 11/11/2023).
31. Doomsday Clock Just Redefined the Entire Multiverse, *CBR*, May 29, 2019.
32. Newton, Casey, *Facebook's CEO on Why the Social Network Is Becoming "A Metaverse Company"*, July 22, 2021, 3 PM, *The Verge*, 10/11/2023.
33. Covell Michele, Bregler Christoph, Cloney Malcolm, *Video Rewrite: Driving Visual Speech with Audio*, Proceedings of the 24th Annual Conference on Computer Graphics and Interactive Techniques, ACM, Digital Library, 19.05.2020.
34. Ahmed F. Moussa, M. Hasna, Z. Jaffal, J. Barafi, *Artificial Intelligence Crimes*, Academic Journal of Interdisciplinary Studies, www.richtmann.org, January 2023.

35. Singh J., Singh P., Kaur R., K.A., Hedabou M., *Privacy and Security in the Metaverse: Trends, Challenges, and Future Directions*, IEEE Access Multidisciplinary, Vol. 13, 2025.
36. Siva K. J., *Social Engineering 2.0: Deepfake and Deep Learning-Based Cyber Attacks (Phishing)*, International Journal for Multidisciplinary Research (IJFMR), www.ijfmr.com, Vol. 07, Issue 1, January-February 2025.
37. Mystakidis, *Metaverse*, Encyclopedia, 486-497. http://doi.org/10.3390/encyclopedia,201031, 2023/11/10.