Chapter 2
Future Cybercrimes in the Metaverse: A Comprehensive Forecast

Ibtesam Mohammed Alawadhi
Dubai Police Academy, UAE

ABSTRACT

In an emerging era of virtual reality, cybercrimes become a significant challenge. The metaverse is a digital realm where people can socialize, work, play, invest, learn, entertain, and much more. The nature of the metaverse raises the concerns of cybercrimes. In this chapter, a deep understanding of potential threats is discussed. Several threats will be highlighted, such as virtual identity theft and impersonation, virtual real estate frauds, malware and ransomware, virtual espionage, advanced phishing, and social engineering. To forecast these threats, insights from cybercrimes are adapted and extrapolated to fit the unique environment of the metaverse. This will guide law enforcement, technical people, policymakers, regulators, and researchers.

1. INTRODUCTION

The term "Metaverse" was introduced in 1992 by Neal Stephenson in his novel Snow Crash (Stephenson, 2003, page number). Neal's definition of the metaverse was a virtual world that humans can interact with for art and commerce. Metaverse is the new digital life where people can entertain, learn, socialize, work, play, and invest. Metaverse also could be identified as virtual worlds partly overlapping with the physical world as the virtual world allows users to be presented as avatars and interconnect with each other (Weinberger, 2022). As the metaverse presents great positive opportunities, it can also be used to perform suspicious activities. Threats in the metaverse differ significantly from traditional threats due to the unique characteristics and complexities of the metaverse. Cybersecurity measures have been developed to indicate known vulnerabilities (Rahman et al., 2022). However, the metaverse introduces new technologies that must be evaluated to eliminate security concerns. Potential threats could include security, privacy, and ethical implications. Generally, those suspicious activities committed in the digital

DOI: 10.4018/979-8-3693-0220-0.ch002

realm are called cybercrime, and they could be committed through unauthorized access, data modification, data interception, or theft of information (Saini et al., 2012). Metaverse applies the new technologies of artificial intelligence, blockchain, and innovation in a platform that offers a whole engagement experience. As people adopt this technology fast, the opportunity for people with malicious intentions arises. Hackers, scammers, and exploiters seek to use any new technology for their gain. It is essential to critically examine the potential threats from using the metaverse and prepare for the new era.

2. PURPOSE

This chapter will discuss cybersecurity challenges to navigate possible risks and put hands on potential threats and vulnerabilities. Furthermore, strategies and countermeasures that should be implemented will also be suggested. Nowadays, we need to collaborate to unify standards and introduce robust security measures to protect individuals and businesses.

3. TYPES OF THREAT ACTORS

Different motivations and capabilities lead to a diverse range of hackers. State-sponsored, cybercriminal organizations and hacktivist groups are different threat actors. State-sponsored hackers are individuals or groups that conduct cyber-attacks like advanced persistent threats for economic, political, military, or other potential purposes (Akoto, 2021). Cybercriminal organizations are identified as hackers who perform illegal activities such as data theft, ransomware, and identity theft to gain profit (Nicolae Sfetcu, 2023). Individual hackers are hackers who perform different types of attacks individually, like unauthorized access, data theft, and disruption of services, and they are also known as black hat hackers (Gerstenfeld, J. 2023). Hacktivist groups are usually motivated by political goals or social agendas and conduct illegal actions like website defacement, denial of service attacks, and data breaches to raise awareness about specific issues (Ulrich et al.; S., 2023).

4. POTENTIAL RISKS

4.1 Virtual Identity Theft and Impersonation

Virtual identity theft and impersonation are the malicious acts of stealing someone's personal information, such as identification numbers, credit card details, and login credentials. Etc. (Popa, Stoklossa and Mazumdar 2023). This act is performed to impersonate the victim later and gain unauthorized access to their accounts to perform suspicious activities, resulting in financial losses, reputation damage, emotional distress, legal repercussions, and trust issues. In the Metaverse, these activities can result in unauthorized access to virtual assets, impersonation of avatars, and misleading communications.