Chapter 5
Predicting Future Cybercrime Trends in the Metaverse Era

Wasswa Shafik
https://orcid.org/0000-0002-9320-3186
School of Digital Science, Universiti Brunei Darussalam, Brunei & Dig Connectivity Research Laboratory (DCRLab), Uganda

ABSTRACT

The Metaverse is a virtual world where users can engage with each other and digital objects in real time, and its usage is growing significantly. However, the rise of virtual environments comes with the risk of cybercrime. This chapter presents the current cybercrime overview in the metaverse by examining recent incidents and standard methods cybercriminals employ. Moreover, it explores factors that could influence cybercrime trends in the Metaverse era, including technological advancements and evolving security measures. Furthermore, it evaluates current and potential cybersecurity measures to prevent or mitigate cybercrime in virtual environments and the importance of user education and responsible online behavior. Finally, we emphasize the need for industry, government, and users to collaborate to mitigate cybercrime in the Metaverse era due to possible negative impacts on social, economic, and environmental settings and its merits benefit people at different levels of endeavors.

INTRODUCTION

The metaverse refers to the theoretical concept of a fully immersive virtual world where users can instantly interact with each other and digital objects (Jaipong et al., 2023). It is a virtual universe that can be retrieved through augmented reality (AR) and virtual reality (VR) devices, enabling users to experience a sense of presence and agency within the virtual environment. The metaverse concept was popularized in science fiction and video games, but it is now becoming a reality due to technological advancements in areas like VR/AR, blockchain, and artificial intelligence (Qamar et al., 2023).

The metaverse is gaining significant popularity due to its potential to revolutionize various industries, including entertainment, education, and e-commerce. For example, the metaverse could transform how people consume and create content in the entertainment industry, enabling more immersive and interac-

DOI: 10.4018/979-8-3693-0220-0.ch005

tive experiences (Seo et al., 2023; Shafik, 2023). For example, concerts, sports events, and theme parks could be recreated within the metaverse, providing users with a unique experience. Furthermore, the metaverse could enhance the learning experience in the education sector by enabling students to interact with virtual objects and simulations, providing a more engaging and practical approach to education. Therefore, in the e-commerce industry, the metaverse could provide new opportunities for businesses to reach customers and offer personalized and immersive shopping experiences (Wu et al., 2023).

However, the increasing popularity of the metaverse also raises concerns about privacy, security, and cybercrime. As more people engage in virtual environments, there is a risk of unauthorized access, data breaches, and other malicious activities (Amalia, 2023). In addition, the immersive nature of the metaverse also makes it an attractive target for cybercriminals looking to exploit vulnerabilities and steal sensitive information. This includes implementing secure authentication methods, such as two-factor authentication and biometric identification, to prevent unauthorized access. It also involves monitoring user behavior and promptly detecting and responding to security incidents (Ariesta & Tuti, 2023). In addition, users must be educated on responsible online behavior, such as avoiding suspicious links and phishing attempts and safeguarding personal information; examples of Tencent's Metaverse are presented in Figure 1.

Figure 1. Tencent's Metaverse, including virtual world and spatial software going mainstream, "premium" social media (more authentic, exclusive, fandom-focused), adoption of decentralized distributed and remote productivity technology, and democratization of e-commerce
(drwealth.com)