EVIDEN

Digital Security Magazine - 12th edition
November 2023

Behind the scenes of Metaverse security: a deep dive into the Social vs. Corporate challenges

By Bartosz Czyzewski

In recent years, the Metaverse has surged in popularity, with an estimated 400 million users in 2022 alone. This dynamic interactive space combines real-life social interactions with extended reality, creating opportunities for entertainment, socializing, commerce, and business activities. As virtual worlds gain traction, ensuring their security becomes paramount.

In this article, we will focus on the analysis of Metaverse use categories and the threats that are affecting them.

33% of developers view data privacy as a major challenge in harnessing the metaverse's potential.

Source: Agora, April 2022

Understanding the Metaverse landscape

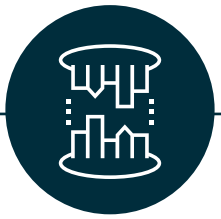
The Metaverse is a multifaceted environment. It encompasses various aspects, from social interactions and public spaces to corporate environments, each serving unique purposes and applications, and also challenges.

#1 Accessing the Social Metaverse

Social or public Metaverse is the place where people converge to converse, play, immerse themselves in art, attend live concerts, and enjoy streaming content. Currently, there are many places where people can "be" after business hours: Decentraland, Sandbox, Hyperverse, not to mention gaming platforms like Fortnite from Epic Games or Roblox.

While some visitors primarily seek specific shows, they often prioritize content over the authorization process. Nevertheless, it's a commonplace occurrence for Metaverse users to create accounts, unlocking a world of possibilities. These include customizing the avatar customization, purchasing and attachment of new items to the character (e.g. NFT's), and, of course, storing credit card credentials.

To facilitate these features, many platforms prompt new members to create a strong password, add a second factor for authentication, or even create crypto-wallet, necessitating the presentation of identity credentials. Notably, the latter authentication method mirrors the security of accessing a bank account.



#2 Accessing the Corporate Metaverse

Distinguishing the Social Metaverse from its Corporate counterpart hinges on contextual application. Within the Corporate Metaverse, we can expect a balance between social engagement, productivity, user-friendliness, creative stimulation, return on investment and cultivating an innovative corporate image. It gets interesting when considering interactions with business partners.

Organizations aspiring to be successful in the Corporate Metaverse should remain mindful of 3 pivotal pillars:

1. Technical capabilities

2. Corporate identities

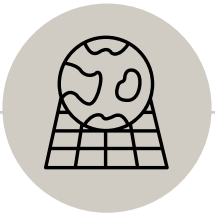
3. Business partners trust relationship

Technical capabilities encompass support for the Metaverse, its users, and the processes intertwined with it. This step assumes paramount importance when structuring the Metaverse, necessitating comprehensive oversight of the diverse use cases it aims to accommodate. Most common corporate use cases are:

Use case	Example
A. Non-technical trainings	Inducting new employees into corporate structures
B. Technical trainings	Providing comprehensive training on new product releases or techniques such as gearbox issues in new vehicle models
C. Business simulation	Assessing user experiences in newly conceived processes or environments
D. Business operations	Allowing Subject Matter Experts or remote workers to observe real-time remote locations and navigating robotic arms or other complex issues
E. Socializing	Engaging in team meetings, gamification, and interactions with external entities
F. Business meetings	Organizing and facilitating innovation workshops and meetings with clients

In the typical corporate scenario (use cases A-E), Central Users Directory (Corporate Identity catalogue) tend to enjoy robust protection, with employees maintaining the confidentiality of their corporate account passwords. Mature organizations may even extend visibility and authorization to external experts, treating them as guests.

However, when orchestrating Metaverse interactions with third-party entities such as Customers or partners (use case "F"), we must plan how to build trust-based connections and relationships. It is especially crucial when important decisions can result from Virtual Reality meetings, a significance amplified in the era of AI and real-time fake identities. Failure to consider cybersecurity can expose organizations to unforeseen additional threats.



#3 Accessing the Business Metaverse

The convergence of Social and Corporate environments: the Business Metaverse

When social and corporate domains converge in the Metaverse, we arrive at the crossroads known as the Business Metaverse. Here, organizations, big and small, venture into the social platforms for business. Regardless of an entity's size, the people representing these organizations are tasked with embodying their company's essence in this virtual realm. These businesses are here to introduce new software, develop new applications, deliver new entertainment content or strategically place ads within the virtual confines of their digital playground.

In this diverse landscape, you'll come across all sorts of professions and roles. For example, an employee might negotiate with a virtual building owner to secure an agreement for ad placement. In this role, they must sign a contract on behalf of their employer. Similar scenarios unfold in the financial sector, where the corporate avatar must be trustful and reliable to ensure successful negotiations. Safeguarding one's identity is critical in this context.

Now, when considering larger organizations with many employees fulfilling similar roles, the challenge of managing business Metaverse identities becomes even more complex. Identity access management tools become necessary to control who is who and who can make some specific operations in the Metaverse.

Summary of general threats

Cyber Threat	Description	Impact on Social Metaverse	Impact on Corporate Metaverse	Impact on Business Metaverse
Weak digital identity	Insufficient digital identity protection that can allow hackers to access a user's account, leading to impersonation (of an individual or organization) and theft of virtual assets.	Lost account control, PII loss, fund loss (NFTs, cryptocurrencies, digital wallets)	Corporate IP loss, sensitive data exposure, corporate privilege abuse, partner trust reduction	Brand reputation loss, financial abuse
Airdrop scams	Unsolicited distribution of fake cryptocurrencies or digital items that aim to steal user funds.	Loss of NFTs, items, cryptocurrencies, digital wallets, user PII	Not applicable	Brand reputation loss, financial abuse
Phishing scams for wallet credentials	Cyber threats using social engineering to steal wallet IDs and credentials.	Loss of NFTs, items, cryptocurrencies, digital wallets, user PII	Brand reputation and IP loss (if digital wallets are used for authentication and authorization)	Brand reputation loss, financial abuse
Fake customer support channel	Attacker mimic of a trusted brand's service like a support channel to gather user information or extort payments.	Account loss, NFT loss, cryptocurrency loss, digital wallet loss, user PII loss	Account takeover, IP loss (data leakage)	Brand reputation loss, financial harm, data exposure, misinformation, manipulation
User impersonation	Pretending to be someone else in virtual avatar interactions, leading to manipulation.	Data leaks, manipulation, misleading information	Corporate trust loss, confidential data leaks, misinformation, manipulation	Loss of brand reputation, financial abuse, leaking confidential data, believing fake information, acting towards a particular intent.
Counterfeit or plagiarized NFTs	Fraudulent NFT copies of digital assets like pictures or artworks sold through fake accounts.	Monetary loss	Not applicable	Reputation damage if fake NFTs are associated with business
Capture of biometric data	Unauthorized collection of sensitive data, such as fingerprints, facial expressions and/or eye/hand movements, by augmented reality and eXtended reality devices, leading to identity duplication for social engineering attacks.	Account loss, NFT loss, cryptocurrency loss, digital wallet loss, user PII loss	Corporate IP loss, sensitive data exposure, privilege abuse, partner trust reduction	Brand reputation loss, financial abuse

Social engineering	Deceptive tactics exploiting trust and psychological manipulation in the metaverse, often resulting in the disclosure of sensitive information or making them susceptible to spying and stalking.	Account loss, NFT loss, cryptocurrency loss, digital wallet loss, user PII loss	Corporate IP loss, sensitive data exposure, misinformation, privilege abuse, partner trust reduction	Reputation loss, corporate IP loss, sensitive data exposure, misinformation, privilege abuse
Replica and fake stores	Shopping in counterfeit brand stores for virtual items. NFTs appear authentic but are owned by the wrong entity due to name similarity (e.g.: like N1ke or Nlke instead of Nike)	Loss of NFTs, cryptocurrencies, digital wallets, user PII	Not applicable	Income loss
Avatar abuse	Obscure behavior and attacks on human dignity, including harassment, stalking, and discrediting.	Social life impact, legal liability	Legal liability	Reputation loss, legal liability

Enhancing Metaverse security

The security of the Metaverse encompasses several critical elements, including legal, compliance, regulations, standards, and technical safeguards.

In the past two years, we have witnessed substantial investments in enhancing the security of metaverse platforms, particularly those supporting metaverse-based transactions. Meta has set the tone by launching substantial bug bounty programs, recognizing the gravity of securing their headsets and metaverse technology. External researchers have actively contributed to these efforts, highlighting a clear commitment to defense. This approach has also been adopted by other platforms in the metaverse ecosystem.

However, vulnerabilities persist. A significant breach on the Metaverse Platform MetaPoint resulted in staggering losses nearing $1 million. Exploiting a smart contract, attackers demonstrated the steep cost of inadequate security measures.

It's time to fortify the metaverse and shape a future where immersive experiences are not only transformative but also secure and reliable.