Think twice before you create an avatar in the metaverse

The online world is slowly evolving into a world - the metaverse, a wholly online reality where people can interact in digital realms using digitised payments, virtual reality and so much more. As Stephen Osler, co-founder and business development director at Nclose, points out, the metaverse is slowly creeping into reality and will soon play a fundamental role in the evolution of business, security and human interaction.

Source: Pexels

The definition of the metaverse has yet to be completely pinned down, it's still a relatively new concept that's being shaped by investment and insights," he adds.

"It's become big news since Meta decided that this was the space in which it would play and, since then, has continued to garner interest and headlines. It's an interesting idea, and an exciting one, but it does ask that organisations and individuals shape their approaches to security to ensure that they're ready for what the metaverse will bring. The idea of living in a complete virtual world is becoming a real possibility where we can interact with others, almost living another life outside of reality, it sounds both exciting but also daunting for cybersecurity."

Even though the metaverse is still in its infancy and more an idea than a usable reality, as it grows there will be vulnerabilities and gaps in its structure that could potentially pose a threat to users and companies.

If it gains traction, it’s going to drive the use of technologies such as virtual reality headsets, digital avatars, cyber-property, non-fungible tokens (NFTs), cryptocurrencies, and smart devices. These are all vulnerable to attack and scam – every, single one.

Real estate in the metaverse is booming

17 Jan 2022

Cybercriminals are already exploiting unexpected weaknesses and human error to dive into systems and access personal and business information at a time when people aren’t wholly immersed in a digital realm. They’re going to be in their element when people suddenly turn digital themselves.

“A virtual reality (VR) and augmented reality (AR) headset can be hacked which means that user-profiles and digital avatars can be stolen or misappropriated in the metaverse,” says Osler. “As people use an increasingly large array of digital devices to access this online landscape, they’re increasing the number of places where they can be hacked. This makes it incredibly important for people to think about how to protect their avatars, devices and information from the outset.”

One of the key challenges facing security within the metaverse is the ability to protect intellectual property and personal information.

Global regulations such as PoPIA and GDRP aren’t able to regulate for what has yet to come, so personal privacy protections and data regulations will ultimately lag behind innovations within the metaverse. It’s also critical to keep in mind that the metaverse is based on a distributed system structure which means that organisations have to be well-versed in personal data protection and how this is handled across different geographical locations and under the supervision of multiple regulatory bodies.

Companies will have to put the ethics of information at the forefront of their engagements within this space; and individuals will have to ensure that they’re protecting their data and systems every step of the digital way.

The metaverse and data privacy: Will regulation keep up?

Ahmore Burger-Smidt 3 Dec 2021

“In addition to concerns around privacy and data, there are questions around other issues such as avatars and cyberland grabs and cybersquatting,” says Osler.

“How will avatars be protected and keyed to their unique user identities? And what about cybersquatters using domain names to hijack legitimate company names and duping people into believing that they’re interacting with a genuine company as opposed to a cybercrime organisation? These are genuine questions that need to be answered to ensure that everyone is protected, right down to the granular level.”

Cybersecurity is going to have to adapt on-demand, pivoting to meet unexpected risks that are only set to increase in veracity and velocity over the next few years.

While there’s no clear roadmap that points to precisely where the problems will be or where the barriers should go up, it’s essential that everyone eyeing the metaverse keeps security at the forefront of their planning and engagements.

“All hardware and software must be secure and up to date with the latest security patches, correctly configured and properly set up,” concludes Osler.

“Data and personal information have to be protected at every corner and every gap filled with robust security protocols and solutions. The metaverse is exciting, it does have potential, but it must equally be tempered by security smarts and intelligent planning.”