It looks like Virtual Reality is back, but are we still blind to its security concerns?

Apple is ready to enter its metaverse era with a mixed-reality headset. The company believes its Vision Pro device will usher in the age of “spatial computing”. In this rush, will we end up unlocking a new era of online fraud? In this article, Tamas Kadar, CEO and cofounder of SEON shares his thoughts on the topic.

Temps de lecture : minute

8 June 2023

Launching early next year, Apple’s Vision Pro mixed-reality headset is certainly dividing opinion among tech commentators and potential buyers. However, within the virtual reality sector, last Monday’s announcement has already been heralded as a ‘watershed’ moment that will help propel the industry into a funding renaissance. It’s a new dawn for a sector that has recently been overshadowed by more significant advancements in the field of generative AI.

Prior to the more recent rise of solutions like Chat-GPT, virtual and augmented reality had widely been considered the ‘future’ of tech. In fact, the rise of the ‘metaverse’ was arguably one of the *big tech trends of 2021*. At the time, leaders in the space, such as Meta Platforms CEO, Mark Zuckerberg had predicted the technology would host a billion people by 2050. Since then, the company’s metaverse-focused Reality Labs division has announced yearly losses of *$13.7B*, which may have somewhat dampened that enthusiasm.

Back to the future

Interestingly, Apple made no mention of the term ‘metaverse’ during its WWDC announcement. This could be to avoid association with previous projects launched by some of the company’s biggest rivals, such as Meta, which relied heavily on that specific term in marketing and that ultimately failed to generate much positive public reaction. Despite this, the Vision Pro solution is broadly the same technological offering as many other metaverse-connected solutions of the past five years.

Widespread acceptance of the metaverse has the potential to bring with it a lot of opportunities. Businesses working in sectors like blockchain, crypto and Web3.0 will see wider spread use and the technology will almost certainly create new revenue streams for those producing digital goods. Unfortunately, alongside these positives the metaverse will almost certainly suffer from many of the cybersecurity and online fraud concerns that plight the internet of today.

Understanding the risks

Let me begin with a very basic fact; fraudsters are always on the lookout for new opportunities to take people’s money. So, it’s a guarantee that bad actors have noticed Apple’s latest announcement and are already calculating how it can be used to facilitate online fraud. Specifically, the launch of Vision Pro will likely generate demand for more socially interactive metaverse projects, which could very quickly become an arena that hosts transactions.

These ‘digital universe’ style metaverse platforms were widely depicted, and often mocked during the first wave of metaverse interest a few years ago. During that period, companies like Meta, Microsoft, and Google were all working on solutions of this nature. If the launch of Vision Pro leads to renewed interest in these platforms, then we may need to be careful as it’s these applications that offer the most abundant avenues for fraud.

The problems we face

Many existing metaverse solutions are vulnerable as they’re unable to stop people establishing more than one account. Having multiple accounts on a metaverse platform could allow fraudsters to take advantage of ‘free credit’, discounts or money back promotions designed for new users. Especially as different metaverse platforms fight for early market share, this form of fraud could quickly become highly problematic as it has across other sectors, such as iGaming.

Metaverse platforms must also watch out for influencer fraud, which has previously affected other major social media platforms. This type of fraud can result in people following fraudulent links or entering sensitive data to enter promotions they believe to be endorsed by well-known, established users. Again, as different platforms vie for early customer adoption, it’s likely that celebrity endorsements will be used as a marketing tactic, which makes this form of fraud a significant issue.

Building defences

Clearly, companies in this space must go to great efforts to ensure their platforms are properly fortified from the earliest launch dates, while also providing users with a frictionless experience. Thankfully, there are methods available to businesses in this field. For one, companies can layer existing defence systems with things like two-factor authentication and machine learning to boot out inauthentic users, bots and high-risk ‘online personalities’.

Enabling browser and *device fingerprinting* can also make a huge difference in preventing fraud in the metaverse. In short, being able to identify someone’s device configuration can help to spot emulators, virtual machines, and bots. Digital footprint analysis also represents a major tool in this battle and can play a role to help verify the validity of accounts by assessing existing social media presence, web platform activity and instant messenger accounts. Data enrichment is an area we specialise in at SEON, so we have first-hand experience of its power in the fight to stop fraud.

The future of fraud?

The announcement of Apple’s Vision Pro has shaken the virtual reality sector and could play a major role in the long-awaited formation of a mainstream metaverse solution. However, it’s still not clear if this is the direction of travel the company plans to take. In fact, early indications point elsewhere, but we must still be prepared. By using the experiences of other industries that have grown immensely over recent years and partnering with the right partners companies it’s an achievable goal.

Tamas Kadar is the CEO and cofounder of SEON.

Article by Tamas Kadar