Survey shows South African employees still believe in the future of the metaverse

According to a recent survey conducted by Kaspersky, a majority of employees in South Africa (61.3%) believe that the Metaverse is the future of the internet and will revolutionise entire industries. Only a few (21.5%) were sceptical of the metaverse and thought that it is a trend that will pass.

SA employees still believe in the metaverse. Source: ThisIsEngineering/Pexels

Kaspersky experts warn that new phenomena like the metaverse bring cyber risks. VR headsets can be attacked to manipulate content, virtual assets earned in the metaverse can be stolen and whole virtual economies compromised.

There are new privacy concerns as well: extensive data about user actions, preferences, and behaviours is collected, which could be exploited for identity theft or surveillance. Protecting individuals' privacy in such a vast and interconnected digital space is a significant challenge.

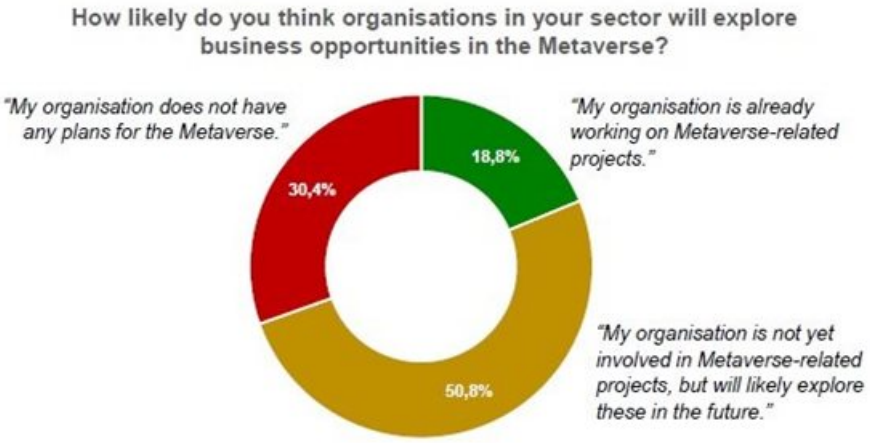
ECOM Africa transforms into Converge Africa

1 Sep 2023

As the Metaverse continues to evolve, cybersecurity strategies will need to adapt to address emerging threats and vulnerabilities.

“When we discuss linking the Metaverse and real-world objects and devices, technically we talk about the rising importance and new roles of IoT in the metaworld. Hence the attractiveness of the ‘Internet-of-Everything’ for global cybercrime increases as well,” comments Victor Ivanovsky, KasperskyOS business development lead.

“This is why IoT vendors should consider implementing a next generation cybersecurity approach on their devices.”



To keep your company protected from cyber threats in traditional and virtual environments, security experts recommend that:

• Organisations should conduct regular cyber skill checkups among employees and offer competent training.

• Corporate users should be educated on potential privacy risks when working in virtual environments. Organisations should implement best practices in safeguarding personal and corporate data.

• Install updates for the firmware used on digital devices (including virtual headsets) as soon as they become available.

• Use a dedicated IoT gateway that ensures inbuilt security and reliability of data transferring.