ความท้าทายการปกป้องตัวตนใน METAVERSE

Metaverse เข้ามามีบทบาทอย่างมากในภาคธุรกิจ **Gartner** คาดการณ์ในปี 2027, 40% ทั่วโลกจะใช้ Web3, Spatial Computing และ Digital Twins เพื่อเพิ่มรายได้ ผ่าน Metaverse จึงเป็นความท้าทายในเรื่องการรับรองความปลอดภัยทางไซเบอร์ของผู้ใช้ เป้าหมายสำคัญคือ การปกป้องตัวตนดิจิทัลใน Metaverse

6 ปัจจัยที่ต้องพิจารณาเพื่อเตรียมดำเนินการ Metaverse

ปรับปรุงกลไกการยินยอม

ผู้ใช้ต้องได้เรียนรู้เกี่ยวกับความเป็นส่วนตัว และกลไกการยินยอมต้องง่าย

ผู้ใช้ต้องรู้เมื่อใดตอบโต้กับ AI

เพื่อความโปร่งใส บอท AI ต้องแสดงตัวตนให้ผู้ใช้ทราบว่ากำลังแบ่งปันข้อมูลกับใคร

การป้องกันข้อมูลส่วนตัวควรใช้งานง่าย

บริษัทควรต่ออายุความยินยอมในทุกจุดที่ป้อนข้อมูลใหม่ แม้จะมีการตรวจสอบสิทธิ์เพิ่มเติมก็ตาม

ความโปร่งใสในการใช้ข้อมูลเพื่อสร้างรายได้

แสดงให้เห็นถึงความโปร่งใสเกี่ยวกับวิธีการใช้ข้อมูล รวมถึงชดเชยให้กับผู้ที่โดนรวบรวมข้อมูล

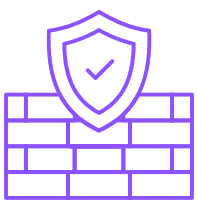
โลก VR ต้องคำนึงถึงความปลอดภัยของข้อมูล

บริการ Metaverse เก็บข้อมูลผู้ใช้จำนวนมหาศาล ดังนั้นแพลตฟอร์มจึงต้องไม่รั่วไหล และใช้หลักการเข้ารหัสที่ปลอดภัย

การควบคุมตนเอง

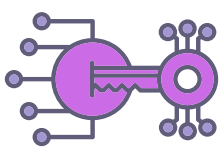
กฎหมายความเป็นส่วนตัวไม่สอดคล้องกันทั่วโลก ว่ากำลังแบ่งปันข้อมูลกับใคร บริษัทต่างๆ จะต้องควบคุมตนเองเพื่อรักษาความไว้วางใจของผู้บริโภค

เทคโนโลยีการรักษาความปลอดภัยของข้อมูล



FIREWALLS

AUTHENTICATION AND AUTHORIZATION



ENCRYPTION

DATA MASKING

HARDWARE-BASED SECURITY

DATA BACKUP AND RESILIENCE

DATA ERASURE

ปัญหาความเป็นส่วนตัวของข้อมูล อาจส่งผลกระทบต่อธุรกิจและผู้ใช้ ดังนั้น ธุรกิจที่กำลังจะก้าวเข้าสู่โลก **METAVERSE** ต้องตระหนักถึงความเป็นส่วนตัวในสองมิติคือ แนวปฏิบัติด้านความเป็นส่วนตัวของเจ้าของแพลตฟอร์ม และนโยบายความเป็นส่วนตัวของผู้ใช้งาน นอกจากนี้การใช้ **Sovereign Digital Identity** ซึ่งอิงตามเทคโนโลยี **Blockchain** จะช่วยให้ผู้ใช้สามารถระบุตัวตนได้อย่างปลอดภัย และไม่ต้องเปิดเผยข้อมูลมากเกินไปด้วย

ที่มา : XR TODAY; Gartner; martechvibe