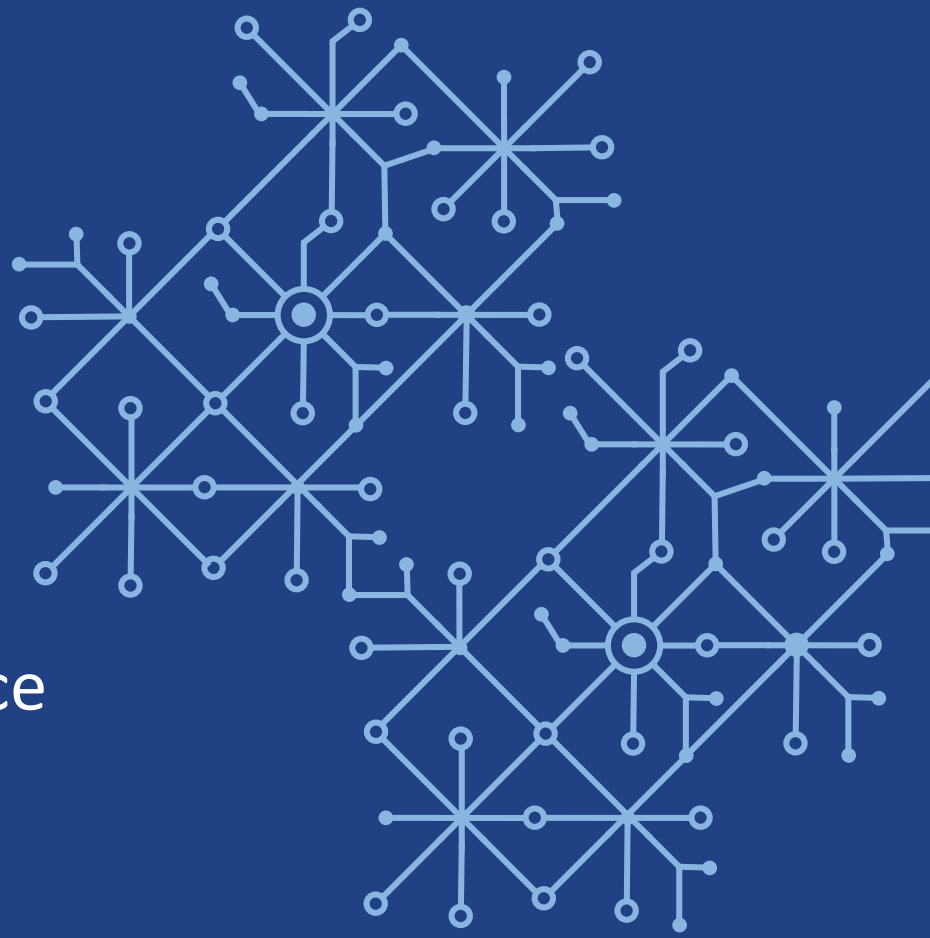
Safety, Privacy, and Accountability in Virtual Worlds

Fabio Maggiore – Head, Cybersecurity Governance



Security and Privacy Risks in the UN Metaverse

The metaverse presents exciting opportunities and applications for the UN:

- UN Executive Briefing on unlocking the potential of virtual worlds and the metaverse for the Sustainable Development Goals
- UNICC is active in the SDG 17: Partnerships for the Goals
- Supporting other UN agencies in achieving their goals.

The metaverse and the virtual worlds applications also bring security and privacy risks:

- Harassment, abuse, and privacy violations are more common in virtual environments.


TECH

Cybercriminals target metaverse investors with phishing scams

PUBLISHED THU, MAY 26 2022•10:22 AM EDT | UPDATED THU, MAY 26 2022•11:36 AM EDT


TECH

A researcher's avatar was sexually assaulted on a metaverse platform owned by Meta, making her the latest victim of sexual abuse on Meta's platforms, watchdog says

Share Save

Weilun Soon May 30, 2022, 7:49 AM GMT+2

Risks in the Metaverse and Virtual Worlds

- **Harassment and abuse:**
  - Virtual environments may involve harassment and abusive behavior, impacting the UN personnel, Partners or beneficiaries.
- **Privacy violations/Identity Theft:**
  - Virtual interactions may compromise the privacy of individuals, leading to data breaches and identity theft.
  - Impersonation and misuse of digital identities within virtual environments.
  - Risk of fraudulent activities and scams targeting beneficiaries and organizations.
- **Data Breaches:**
  - Unauthorized access to sensitive personal and organizational data.
  - Potential exploitation of vulnerabilities in metaverse platforms to steal or manipulate data.
- **Cyber Attacks:**
  - Increased attack surface with interconnected virtual environments.
  - Potential for DDoS attacks, malware, and phishing schemes targeting metaverse users.
- **Content Manipulation:**
  - Spread of misinformation and deepfakes.
  - Manipulation of virtual content to mislead or harm users.

These risks can damage UN system reputation and affect the achievement of UN goals.

Possible Safeguards

- **Traditional Cybersecurity** and **Data Protection frameworks** (e.g. ISO 27001, ISO 27701, SOC2) and controls are still relevant and mostly applicable to metaverse and virtual worlds.
    - Cybersecurity and Privacy policies
    - End user awareness
    - Identity and access management
    - Encryption
    - Content verification tools
    - Risk assessments
    - Inventory, asset management, patch management
    - Etc.
- Employ **blockchain-based** initiatives such as the UN Digital ID providing a secure and trusted digital identity for UN personnel and partners.
    - by enforcing policies and standards to prevent harassment, abuse, and privacy violations in virtual environments.
    - by ensuring secure access to UN systems and platforms, including metaverse and virtual worlds applications.

Thank you!

Digital.
For the UN family