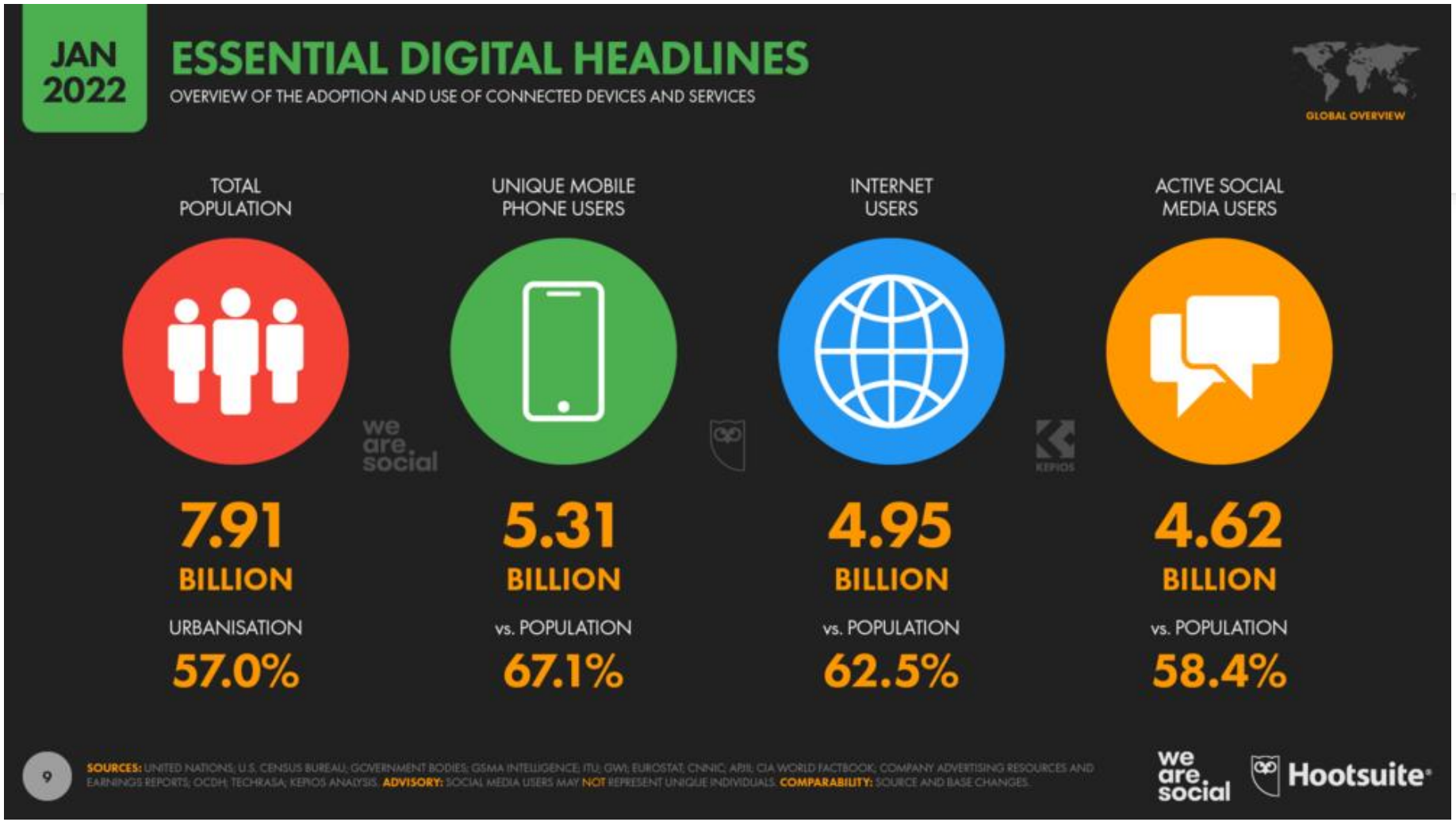
Cybersecurity flaws in the Metaverse #1

Joas Antonio

https://www.linkedin.com/in/joas-antonio-dos-santos


JAN 2022
ESSENTIAL DIGITAL HEADLINES
OVERVIEW OF THE ADOPTION AND USE OF CONNECTED DEVICES AND SERVICES
GLOBAL OVERVIEW
TOTAL POPULATION
UNIQUE MOBILE PHONE USERS
INTERNET USERS
ACTIVE SOCIAL MEDIA USERS
we are social
KEPIOS
7.91 BILLION
5.31 BILLION
4.95 BILLION
4.62 BILLION
URBANISATION
57.0%
vs. POPULATION
67.1%
vs. POPULATION
62.5%
vs. POPULATION
58.4%
9
SOURCES: UNITED NATIONS; U.S. CENSUS BUREAU; GOVERNMENT BODIES; GSMA INTELLIGENCE; ITU; GWI; EUROSTAT; CNNIC; APJII; CIA WORLD FACTBOOK; COMPANY ADVERTISING RESOURCES AND EARNINGS REPORTS; OCDH; TECHRASA; KEPIOS ANALYSIS. ADVISORY: SOCIAL MEDIA USERS MAY NOT REPRESENT UNIQUE INDIVIDUALS. COMPARABILITY: SOURCE AND BASE CHANGES.
we are social
Hootsuite

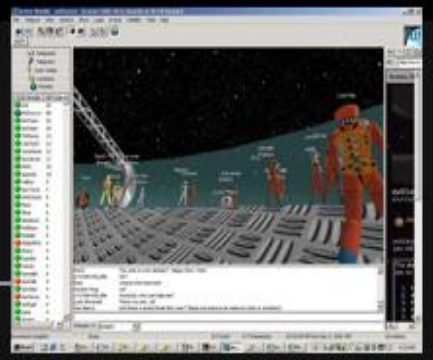
Emerging Technologies in 2022 and 2023

- Smart Spaces: Enhancing the capability of spaces using IoT and AI;
- Generative AI: Creation of new materials, based on original data, example: Thisdoesnotexist and other AI that can even generate texts, audios and images;
- Metaverse: In 2022 refers to the merging of video games, social media and entertainment to create new immersive experiences, like swimming into your favorite music at an online concert.

What is Metaverse?

- The Metaverse can be described as a 3D version of the Internet being an interconnected system that transcends national borders. Therefore, it will be necessary to define a network of public and private standards, norms and rules to operate in all jurisdictions.
- The metaverse will be a constellation of technologies, platforms and products. Not just one, but all. And that takes a number of companies large and small, society, the public sector and millions of individual creators.

'Back to the Future Part II'



Active Worlds

Second Life

Jogador Nº1

Facebook horizon

1989

1992

Book Snow Crash

1995

2000

Habbo

2003

2011

Jogador Nº1

2018

2020

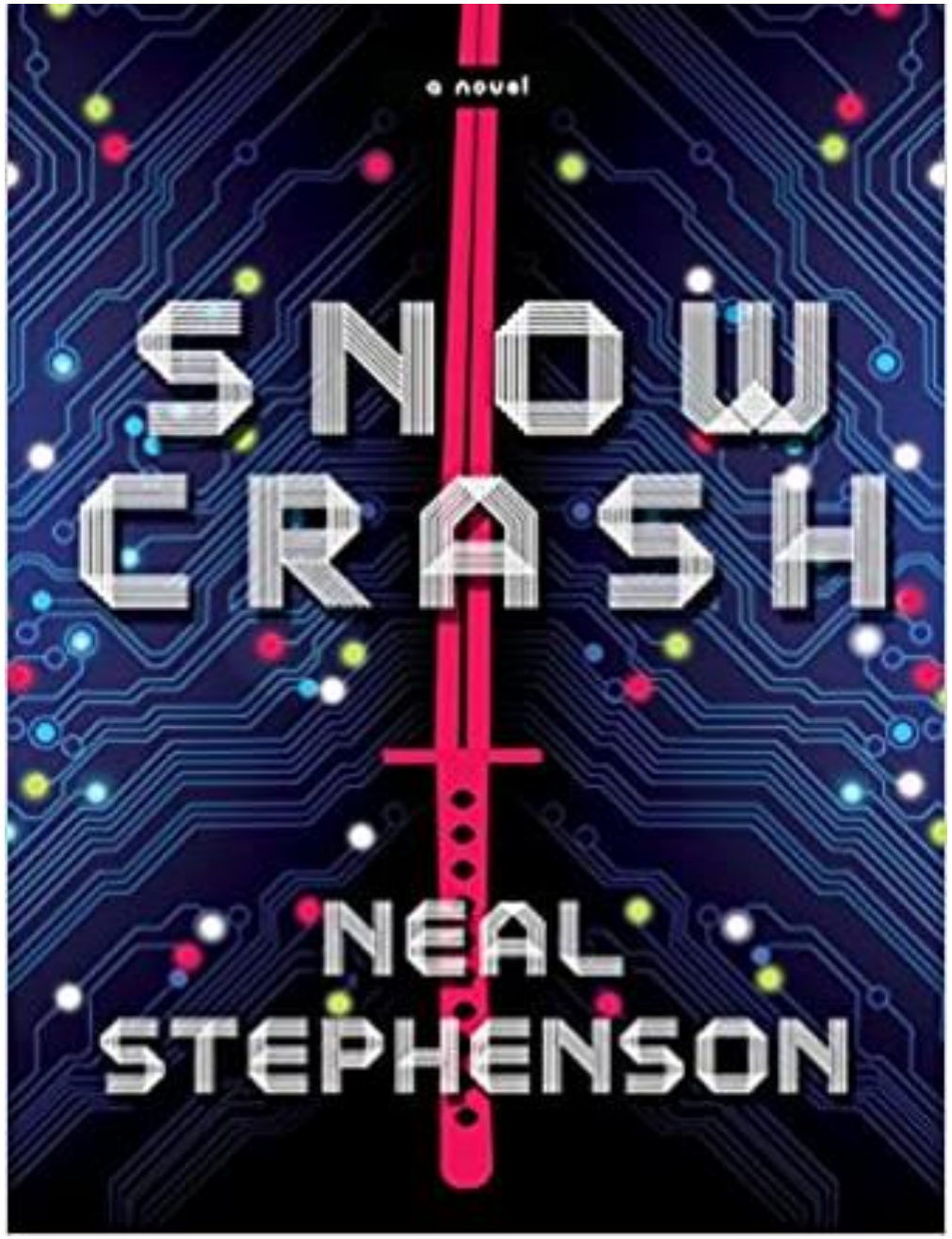
UPLOAD

2021

CREDITS BY CLEBER SOARES

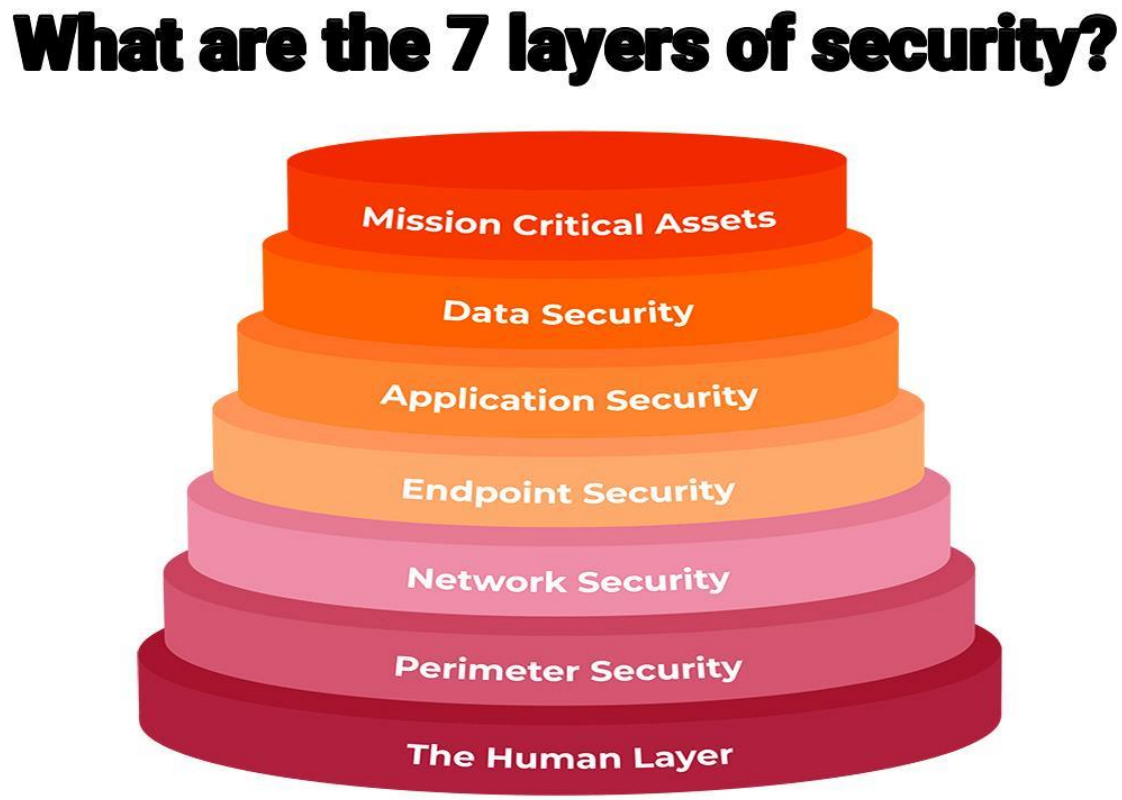
Snow Crash - Origin

- “The word 'metaverse' was actually coined by author Neal Stephenson in his 1992 science fiction novel Snow Crash. In his book, Stephenson referred to the metaverse as an overarching digital world that exists parallel to the real world.”



Metaverse Risks

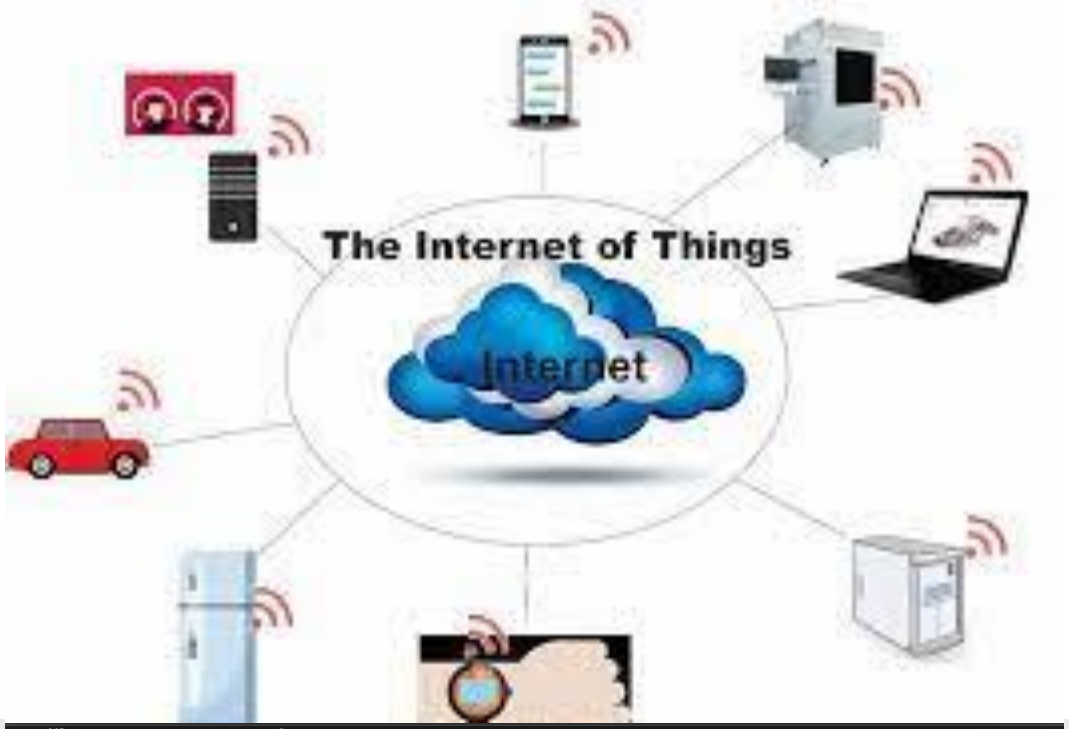
- Physical Security
- Network Security
- System Security
- Application Security
- User Security



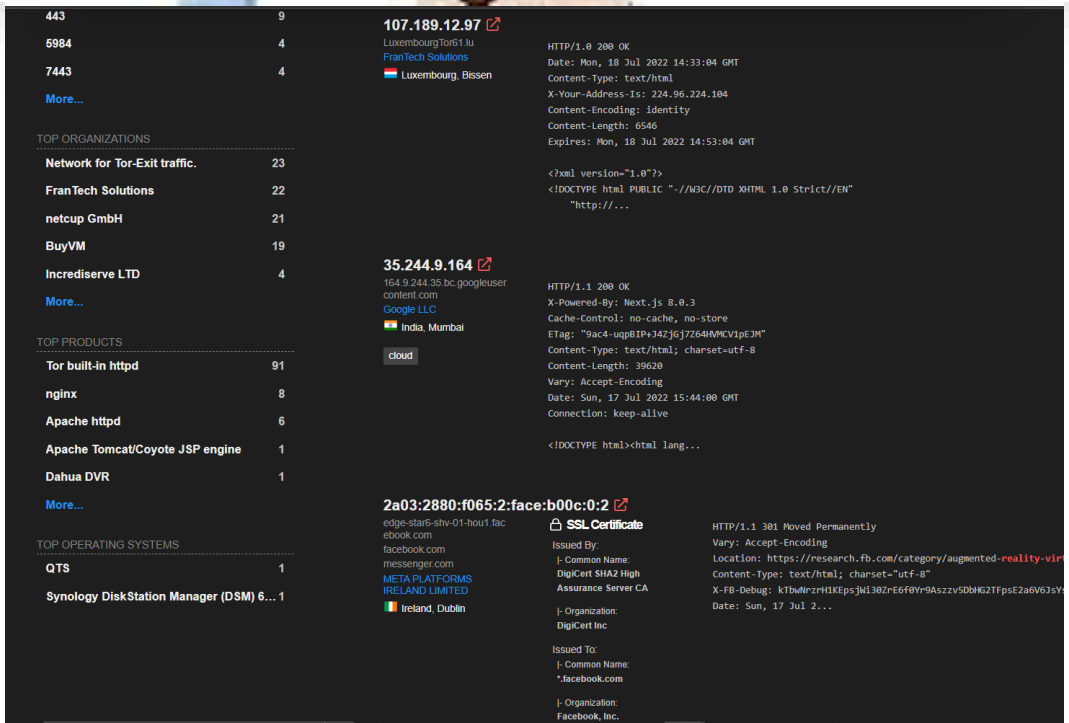
Physical Risk

- “With what we have today, is it possible to be immersed for a few hours in a world that will trick our brain to the point of no longer recognizing what is outside the lens?” No!
- Headaches, Nausea, disorientation and other symptoms end up being a reality in the current metaverse;
- Users typically move around in the real world with an Augmented Reality overlay, making physical safety a concern. If users get too immersed in the virtual world, they can harm themselves or those around them.

Network Risk

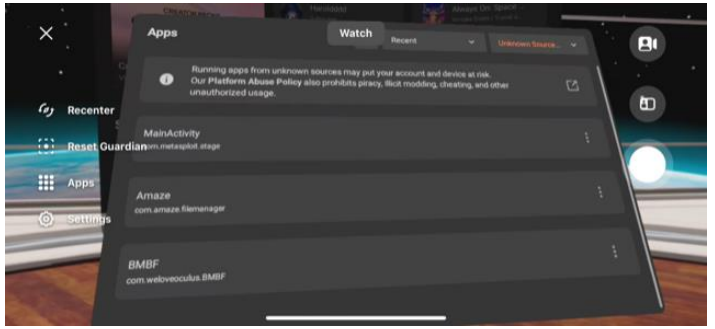


- Improperly opened ports and services;
- Traffic on unsafe websites;
- Lack of network security (Segregation of VLANs, use of secure protocols, tools such as DLP, Zero Trust, Firewall, etc.);
- Devices and development environments exposed to the Internet;



System Risk

Command	Requires	Notes
`continue`	-	-
`reboot`	-	-
`reboot-bootloader`	-	-
`oem device-info`	-	displays information about the device
`oem reboot-edl`	-	allows to reboot into emergency download mode
`oem reboot-sideload`	-	allows to reboot into sideloading mode
`oem shutdown`	-	shuts down the device
`getvar`	-	-
`oem sha1`	-	computes the hash of a partition
`oem unlock`	-	unlocks the device
`oem lock`	-	locks the device
`flash`	-	-
`erase`	-	-
`oem partition-info`	-	list the partitions
`boot`	DU or CU	-
`oem select-display-panel`	DU or CU	-
`oem set-verity`	DU or CU	enables/disables dmverity
`oem set-verified-boot`	DU or CU	enables/disables verified boot
`oem get-kernel-flavor`	DU or CU	get the kernel flavor




```
meterpreter > sysinfo
Computer    : localhost
OS          : Android 10 - Linux 4.19.81+ (aarch64)
Meterpreter : dalvik/android
meterpreter >
```

CVE-2018-9568_WrongZone	cve-2018-9568: fix link to firmware	3 years ago
CVE-2019-2215_BinderThreadUaf	Update readme.md	3 years ago

- VR Glasses Kernel Exploration;
- Android Reverse TCP;
- Running OEM Fastboot commands;
- Install third-party applications;

https://github.com/QuestEscape/research

Application Risk

- Vulnerabilities in BlockChain platforms;
- Risks with NFT;
- Lack of secure development in applications;
- Lack of integrity, availability and confidentiality in certain applications;
- Abusive terms of use;
- Vulnerabilities in the Client (Reverse Engineering in Glasses);

Application Risk #2

- “An example occurred with the company Sky Mavis. In which an attacker used compromised private security keys to break into the network nodes that validate inbound and outbound transfers to the Ronin blockchain. This allowed the attacker to silently withdraw large amounts of Ethereum.”
- Extra: These tokens are powered by smart contracts, which in turn are deployed as compiled code within a transaction on the blockchain. And as “non-fungible” as the tokens themselves may be – meaning that their representation within the blockchain is unique and cannot be duplicated – the metadata associated with NFTs is very fungible. Therefore, nothing prevents copycats from creating new NFTs (using different smart contracts, or even different blockchains) that point to a copy of the content associated with the original.
- Another recent technique used by attackers is offering malicious tokens through so-called airdrops. Since wallet addresses are public, literally anyone can send NFTs to these addresses.

User Risk

- Phishing Attacks;
- Identity theft;
- Privacy of data entered on the platform;
- Understand the concept of smart contracts to identify whether the source code is published or not;
- Identity management;
- Harassment and verbal aggression;
- Deepfakes;
- Malware attacks;

Metaverse users' identities can be spoofed, their accounts can be hacked, and their avatars can be controlled. A common challenge is that the identity of the person metaverse users are dealing with is always questionable.

What's your choice: Reality or Simulation?

THANKS!

SCAN ME