



# Safeguarding the Virtual Space

Komal Agarwal

---

# What is Virtual space

- Digital environments where users interact with each other and with digital content.
  - A digital world extending beyond traditional physical and social realms.
  - Includes the World Wide Web, the Internet, and global media/communication channels.
  - A social media platform, any online gaming platforms, virtual office spaces, virtual reality platform, etc.
- 



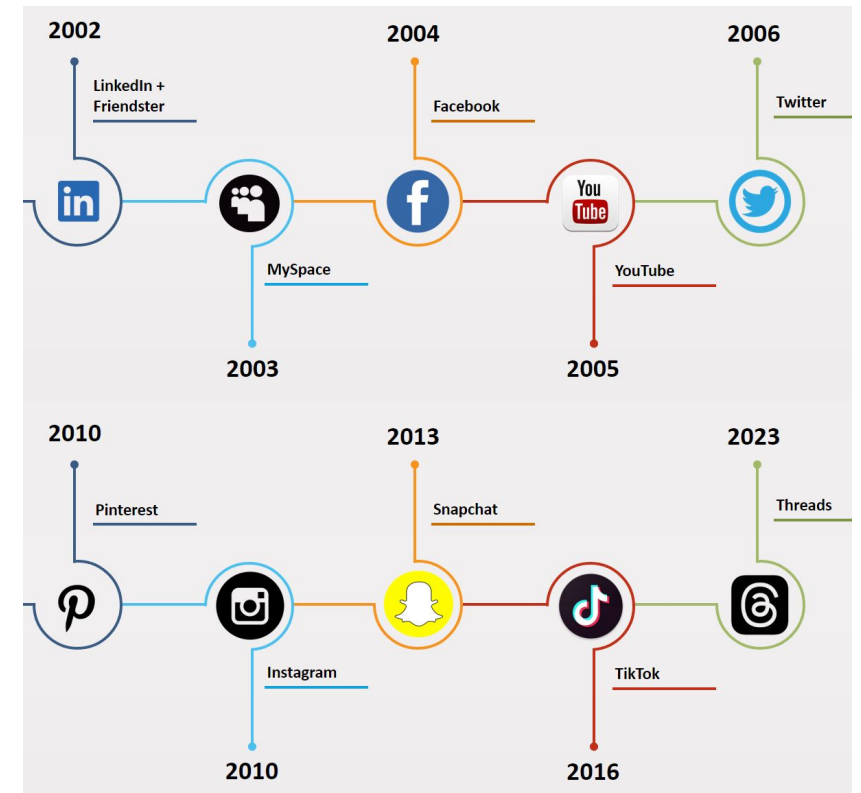
# Characteristics of Virtual Space

- Digital, virtual, abstract, and time independent.
  - Comprises globally connected networks of computers and related infrastructures.
  - It is integrated into daily life for work, education, socializing, and entertainment.
  - It connects people across continents in real-time, transcending physical boundaries.
  - Virtual spaces are not just a part of our lives; they are shaping how we learn, work, and connect with each other
- 



# Evolution with Web 2.0 and User Generated Content

- Shift from passive spectatorship to active participation in digital spaces.
- Users can now modify and create digital content collectively.
- Rise of social media applications for content creation, information exchange, and community building.

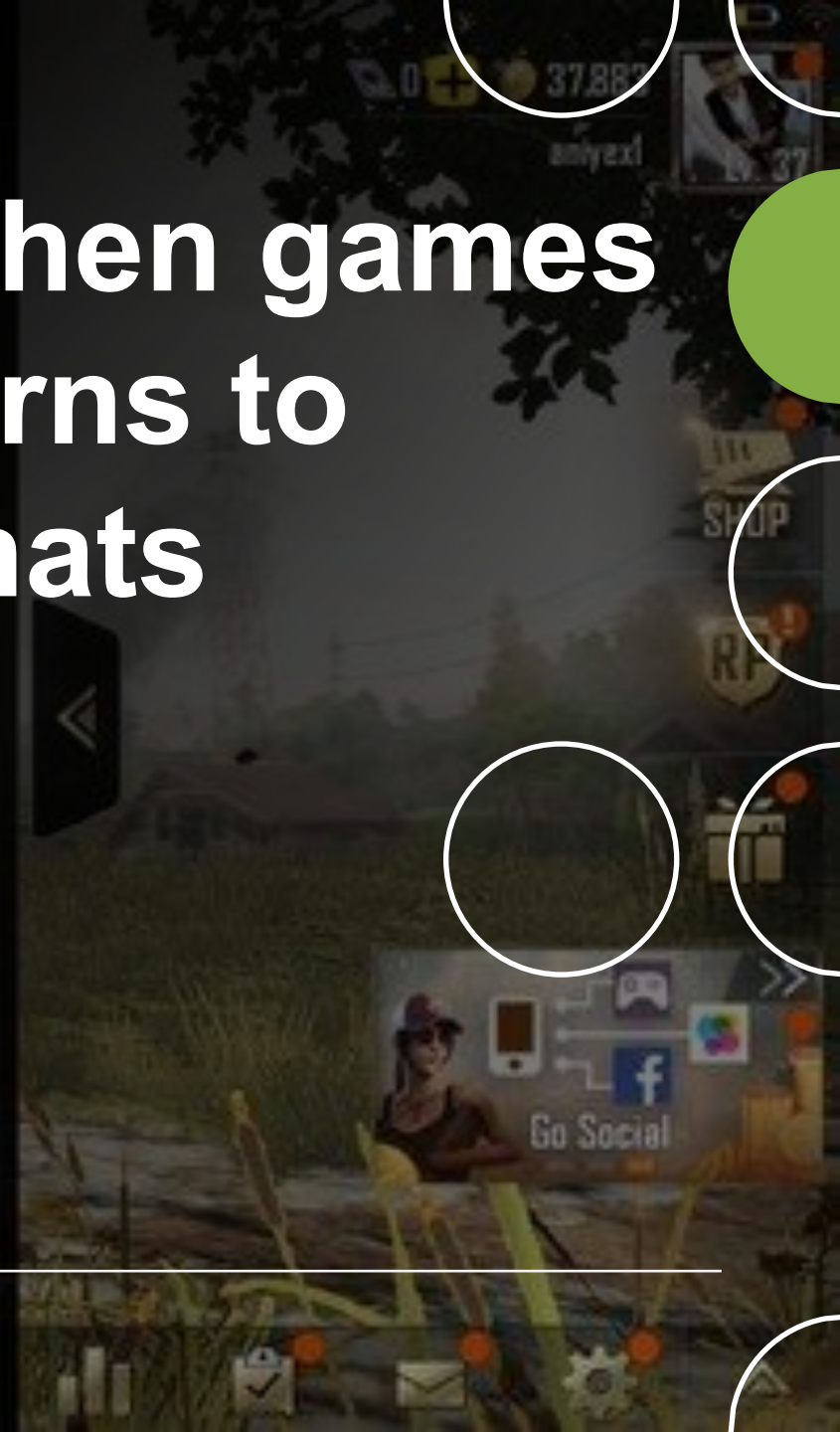


# Virtual Space and Daily life

- Integral for learning, business, socializing, and personal identity development.
  - Interweaves 'real' life with virtual environments through continuous information and interaction.
  - Digital technologies, including smartphones, become extensions of physical selves.
-



When games turns to chats



# Modern day boardrooms




# Vision Pro


Video credits: Apple Inc.




Shop from  
anywhere  
while sitting  
at home



NFT  Karli Kloss - Parka Jacket



Voucher for Physical Item & Digital Asset

	<b>Parka Jacket</b> x1	US\$ 3000.00
<small>Sold by: The Fabricant</small>		<small>5.300745 Eth</small>
<small>Made by: Adidas x Karli Kloss</small>		

[Buy](#)

# The threats in Virtual Space

- Cybersecurity Threats:
    - Hacking: Unauthorized access to personal or business data. Hackers can steal sensitive information, disrupt services, or even take control of devices.
    - Phishing Scams: Deceptive attempts to obtain sensitive data (like login credentials) by masquerading as a trustworthy entity in electronic communications.
    - Malware and Viruses: Malicious software intended to damage or disable computers and systems, often spread via email attachments, software downloads, or compromised websites.
-

< > EGIFNIKMRJKWIAESAWEBRZFGVJAENBNTYNY\_2023-10-18 13-40-15

Name

> Autofills

> Cookies

DomainDetects.txt

ImportantAutofills.txt

InstalledBrowsers.txt

InstalledSoftware.txt

Passwords.txt

ProcessList.txt

UserInformation.txt

This is what a stealer malware collects from the victim's system.

URL: https://[redacted]gin  
Username: sms[redacted]  
Password: sem[redacted]  
Application: Google\_[Chrome]\_Default  
=====

URL: https://www.orange.co.uk/business/myaccount/login  
Username: 6[redacted]  
Password: fr[redacted]  
Application: Google\_[Chrome]\_Default  
=====

URL: https://w[redacted]  
Username: malak[redacted]  
Password: yzbE[redacted]  
Application: Microsoft\_[Edge]\_Default  
=====

URL: https://w[redacted]sword  
Username: smsm[redacted]  
Password: Semo[redacted]  
Application: Microsoft\_[Edge]\_Default  
=====

URL: https://accounts.hsoub.com/settings  
Username: UNK[redacted]  
Password: Fp[redacted]  
Application: Microsoft\_[Edge]\_Default  
=====

URL: https://id[redacted]  
Username: UNKN[redacted]  
Password: Semo[redacted]  
Application: Microsoft\_[Edge]\_Default  
=====

URL: https://rsc.mped.gov.sg/Identity/Account/Register  
Username: sam[redacted]  
Password: Semo[redacted]  
Application: Microsoft\_[Edge]\_Default  
=====

URL: https://s[redacted]  
Username: smsm[redacted]  
Password: W[redacted]  
Application: Microsoft\_[Edge]\_Default  
=====

URL: https://www.orange.co.uk/business/myaccount/Captcha-Login  
Username: 53[redacted]  
Password: fr[redacted]  
Application: Microsoft\_[Edge]\_Default  
=====

URL: https://e[redacted]  
Username: WEST[redacted]  
Password: Semo[redacted]  
Application: Microsoft\_[Edge]\_Default

- Privacy Concerns:

- Data Theft: Unauthorized access and theft of personal data which can lead to identity theft or financial loss.
  - Surveillance and Tracking: Users can be tracked online, leading to a loss of privacy. Companies or individuals can collect data on online activities, sometimes without consent.
  - Inadequate Data Protection: Many platforms may not have robust data protection measures, leaving user data vulnerable.
-

- **Social Risks:**

- **Cyberbullying:** The use of digital platforms to harass, threaten, or embarrass individuals. It's particularly prevalent among young people.
  - **Online Harassment:** Includes stalking, trolling, and other forms of harassment that can lead to emotional distress.
  - **Misinformation and Fake News:** The spread of false information can lead to confusion, panic, and in some cases, dangerous situations.
-

- **Addiction and Mental Health Issues:**
    - **Internet Addiction:** Excessive use of the internet which can impact daily life, relationships, and physical health.
    - **Impact on Mental Health:** Overuse or negative experiences online can lead to issues like depression, anxiety, and low self-esteem.
-

- Content Risks:

- Inappropriate Content: Exposure to harmful or inappropriate content like violence, adult content, or hate speech.
  - Predatory Behavior: Predators may use virtual spaces to exploit or groom unsuspecting individuals, particularly minors.
-

- **Economic Risks:**

- **Financial Frauds:** Scams aimed at financially exploiting users, such as fake investment schemes or fraudulent online shopping sites.
  - **Intellectual Property Theft:** Unauthorized copying, sharing, or use of copyrighted material, including software, music, and video.
-



- Legal and Regulatory Risks:
    - Non-compliance with Laws: Users or companies might inadvertently violate laws, such as those related to copyright or data protection.
    - Jurisdictional Issues: Legal complexities when disputes involve parties in different countries.
-

# A case study – Wearable Technology

- Background Scenario:
- A person is sitting opposite you, equipped with smart glasses that have the capability to capture images of whatever the wearer is looking at.



- Privacy Concerns:
  - Consent for Image Capturing: There is no clear indication to bystanders when an image is being taken, raising concerns about consent.
  - Notification of Recording: Unlike traditional cameras that have a visible flash or sound, smart glasses may not provide any notification to those being recorded.

#### Potential Risks:

- Invasion of Privacy: Unconsented recording can lead to personal information being captured and potentially misused.
  - Data Security: Images taken could be stored in a cloud service, raising questions about data security and vulnerability to hacking.
  - Misuse of Information: Photos taken without consent could be used for malicious purposes, such as surveillance or blackmail.
-

- **Legal and Ethical Implications:**

- **Lack of Regulation:** There may be a lack of clear legal frameworks specifically addressing the use of such devices in public or private spaces.
- **Ethical Use:** The ethical guidelines governing the use of such technology are not always clear or universally accepted.

- **Detection and Prevention:**

- **Indicator Signals:** Some smart glasses have an indicator light that turns on when recording, but it may not be noticeable.
  - **Technology Detection:** Development of counter-technologies that can detect and signal the use of recording devices in the vicinity.
  - **Policy and Procedure:** Establishing policies in certain environments (like locker rooms or private meetings) where such devices are not allowed.
-

- What privacy rights are potentially being violated in this scenario?
  - How effective are current laws in protecting individuals from such privacy invasions?
  - What technological or policy measures could be implemented to prevent unauthorized recordings?
  - How does the right to privacy balance with the freedom to use wearable technology?
-

**Are we  
seeing the  
real  
individual?**

---



# The frauds getting advanced these days

## Man Scammed by Deepfake Video and Audio Imitating His Friend

A man in China lost 4.3 million Yuan after receiving a video call from a scammer who used AI software to replicate the face and voice of his supposed friend.

## Man scammed out of Rs. 40000 via AI-based video call on WhatsApp; know how to catch deep fakes

On July 16, Artificial Intelligence-based, deep fake technology, tools were utilized in WhatsApp video calls, defrauding a man of Rs. 40000.

By: HT TECH | Updated on: Jul 17 2023, 11:32 IST

## Kerala Man Loses ₹ 40,000 To AI-Based Deepfake Scam: Here's What It Is

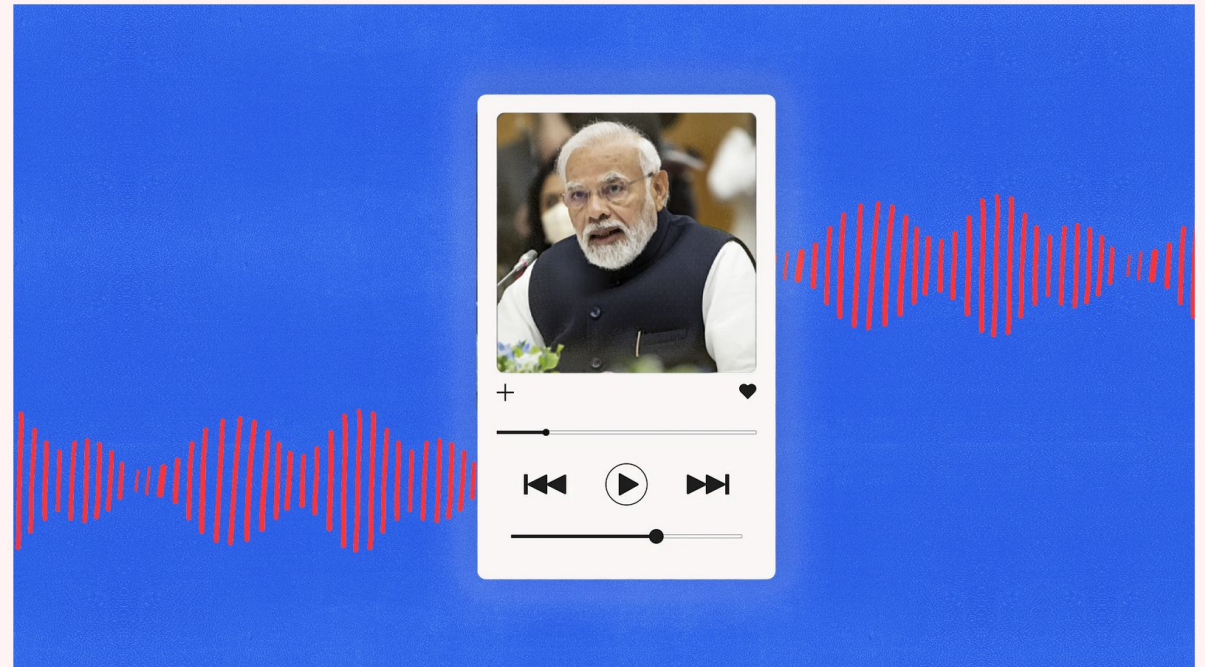
A man in Kerala's Kozhikode lost ₹ 40,000 after falling prey to an artificial intelligence-based scam. According to the police, it was a deepfake scam involving someone who the man knew.

India News | Edited by Amit Chaturvedi | Updated: July 18, 2023 1:43 pm IST

**Do you believe if  
you hear our  
Prime Minister  
singing "Chaleya"  
Song in  
Instagram?**

## **AI Modi started as a joke, but it could win him votes**

AI-generated songs, like the ones featuring Prime Minister Narendra Modi, are gaining traction ahead of India's upcoming elections.



Rest of World/Getty Images



# Imagine the following scenario

- You get a video call from your friend; he is in despair. He said that his family member is admitted in a hospital due to an accident.
  - He asks you for some financial help. What will you do?
  - How many of you will check if its really your friend? How can you confirm?
  - How many of you will check if it is his real number?
  - Did his accent or gestures change?
-

# When we use insecure network and visit sites without SSL (https)

The image shows a Wireshark packet capture window titled "Wireshark · Packet 402 · http password.pcapng". The main pane displays the details of an HTTP request. The request headers include:

- Accept-Language: en-US,en;q=0.5\r\n
- Accept-Encoding: gzip, deflate\r\n
- Content-Type: application/x-www-form-urlencoded\r\n
- Content-Length: 36\r\n
- Origin: http://testphp.vulnweb.com\r\n
- Connection: keep-alive\r\n
- Referer: http://testphp.vulnweb.com/login.php\r\n
- Upgrade-Insecure-Requests: 1\r\n

The request body is shown as "HTML Form URL Encoded: application/x-www-form-urlencoded" and contains two form items:

- Form item: "uname" = "vijaymehta"
  - Key: uname
  - Value: vijaymehta
- Form item: "pass" = "maxelladiviner"
  - Key: pass
  - Value: maxelladiviner

The packet list pane on the right shows the following details for the selected packet:

- 1232 Len=0 TSval=773377641
- .251 for any sources
- 63488 Len=0 TSval=216347700
- Win=64128 Len=0 TSval=2163
- 31232 Len=0 TSval=773377813
- Win=31232 Len=0 TSval=7733
- 64128 Len=0 TSval=216347868
- .255.250 for any sources
- .251 for any sources
- 1

# How to be safe?

- Use a VPN (genuine and trusted) for doing transactions or while communicating sensitive information in an unsecured public network.
  - Use genuine devices like VR Headsets or smart glasses.
  - Make sure to turn off Bluetooth and Wi-Fi hotspots in not in use.
  - Secure your Wi-Fi network using strong password and security algorithms.
  - Do not post sensitive information or personal information on public chat rooms or gaming forums.
  - Make sure to identify the caller before performing any financial transactions over the telephonic call or video call.
  - Use a genuine and trusted anti-virus for the devices.
-

# Majority of the scams or threats in Virtual Space arise due to lack of adequate knowledge

- Since many of the users start to use these platform out of curiosity. They might not be aware of the security configurations they have to make before using these.
  - When we use the default configuration or default privacy settings there is high chances that this will be vulnerable to attacks.
  - Understanding the platforms or devices we use is really important to make ourselves safe in the virtual space.
-

# Sharing Personal information

- As we saw, the rise of AI has resulted in many new concerns to privacy and threats.
  - Make sure the information you share online is not being a double-edged sword.
  - Do not disclose any sensitive or personal information online.
  - Make sure to keep your photos private, or restricted.
  - Do not share any sensitive information to the strangers we meet in public/online platforms.
-

An aerial photograph of a multi-lane highway bridge spanning across a body of turquoise water. The bridge has several lanes in each direction, with white lane markings and a central divider. Several vehicles, including cars and trucks, are visible on the bridge. A large black rectangular box is overlaid on the right side of the image, containing the text "Thank You & Stay Safe" in white. The background is a vibrant turquoise color with decorative white circles and a solid green circle on the right side.

**Thank You &  
Stay Safe**