



ऑनलाइन प्रशिक्षण “साइबरस्पेस में उभरती चिंताएँ”

केंद्रीय शैक्षिक प्रौद्योगिकी संस्थान, एनसीईआरटी, नई दिल्ली द्वारा आयोजित

दिन 5: सोशल मीडिया सुरक्षा

मेजर विनीत कुमार
संस्थापक एवं वैश्विक अध्यक्ष,
साइबर पीस फाउंडेशन

के साथ सीधा संवाद

Introduction



India boasts over **806 million** internet users, with a significant portion active on platforms like Facebook, Instagram, and WhatsApp.



While specific data on internet usage among children and young adults in India is limited, global trends provide some insight. Globally, **19% of internet users are aged 18 to 24**. Applying this percentage to India's internet user base suggests that approximately **153 million users** are within this age group.



As of early 2025, India has approximately **806 million** internet users, representing **55.3% of the population**. Projections indicate that this number is expected to surpass **900 million** by the end of the year, with **rural areas accounting for 55% of users**.

This growth is largely driven by the increasing availability of digital content in regional languages.



Introduction



Children **under 18 constitute about 14%** of India's overall internet user population. This equates to approximately **113 million users** under 18 years old.

Therefore, combining these estimates, around **266 millions** of India's internet users are children and young adults aged 24 and below.



FEB
2025

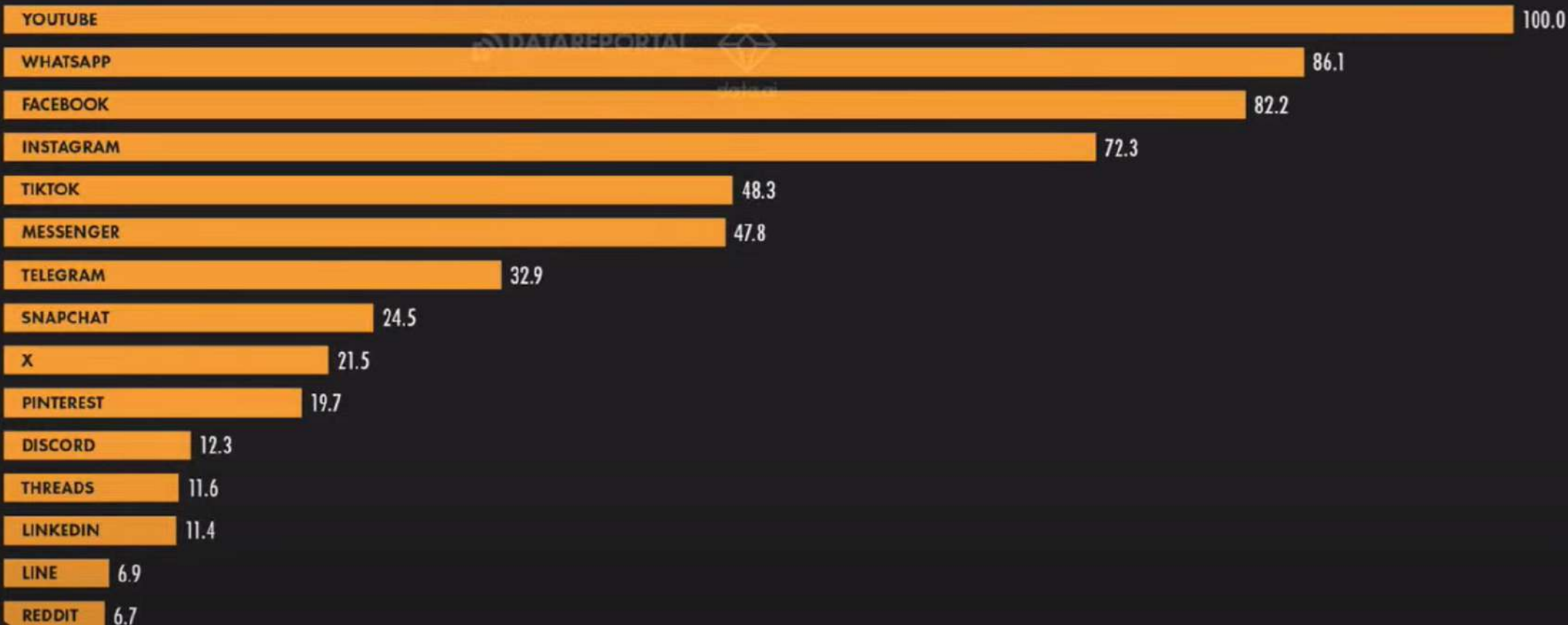
SOCIAL MEDIA APPS: ACTIVE USER INDEX

INDEX OF THE NUMBER OF SMARTPHONE HANDSETS USING EACH PLATFORM'S MOBILE APP IN NOVEMBER 2024

Sign in



GLOBAL OVERVIEW



SOURCE: DATA.AI (A SENSOR TOWER COMPANY). **NOTES:** BASED ON A SELECTION OF APPS ONLY. DATA IS NOT AVAILABLE FOR APPLE IMESSAGE. FIGURES BASED ON MONTHLY AVERAGE NUMBER OF IPHONE AND ANDROID PHONE HANDSETS ON WHICH EACH PLATFORM'S MOBILE APP WAS OPENED IN NOVEMBER 2024. VALUES ARE AN INDEX OF EACH PLATFORM'S AVERAGE MONTHLY ACTIVE USERS FOR THE STATED PERIOD COMPARED WITH USERS OF THE TOP APP DURING THE SAME PERIOD. DOES NOT INCLUDE DATA FOR CHINA. **COMPARABILITY:** VALUES ARE BASED ON SMARTPHONE HANDSETS, NOT UNIQUE INDIVIDUALS OR ACTIVE USER ACCOUNTS. NOTE THAT SOME INDIVIDUALS MAY USE MULTIPLE HANDSETS, WHILE SOME HANDSETS MAY ACCESS MULTIPLE USER ACCOUNTS.

we
are
social

Meltwater

Emerging Concepts Emerging Technologies



Cyber Security Threats

Phishing

Ransomware

Hacking & Data Breaches

Distributed denial of Service

Cyber War



Data Privacy & Security

Financial Frauds

Lottery Scams

Cyber Bullying

Dating Scams



Online Fraud Abuses

Data Sharing & Ownership

Access to sensitive Information

Misuse of Data & Breach of Privacy

Reputation damage

Ethical Concerns



Anti-Competitive Conduct

Monopolization

Manipulation of search results

Bundling of apps, abuse of Data

Collusion in online Advertising

Big Data & Algorithms - tacit Collusive Agreements



Abuses on Social Media

Identity Theft

Stalking

Misinformation & Disinformation

Threat to Public trust and Social harmony

Social Engineering



ONLINE THREATS TO CHILDREN & YOUNG PEOPLE



**CHILD SEX
PREDATORS**



**CYBER BULLYING
SEXTORTION**



**ACCESS TO
INAPPROPRIATE CONTENT**



**CHILD SEXUAL ABUSE
MATERIAL**



**LIVE STREAMING AND ON
DEMAND SERVICES
SEXTORTION**



**COMMERCIAL SEXUAL
EXPLOITATION AND
TRAFFICKING**



**CHILD SELF-GENERATED
SEXUAL CONTENT**



**ONLINE GAMING
ELECTRONIC ADDICTIONS**

Online Harassment



Lewd comments or remarks



Trolling

Forceful sexual conversation



Sending objectionable images



Sending spam links



Cyberbullying & Online Harassment



Cyberbullying and online harassment are serious ethical issues that can have severe consequences.



It involves the use of digital communication tools to intimidate, threaten, or humiliate others.



As responsible digital citizens, it is our duty to prevent and address these problems.



If you encounter cyberbullying or online harassment, report it to the appropriate authorities and support the victims.

Phishing, Smishing & Vishing

01

Phishing: Phishing is one of the most common forms of fraud, where scammers use a seemingly real email address with a link that urges you to input information like your full name, social security number, and credit card number.

02

Smishing: Smishing uses text messages or common messaging apps, like Slack, to contact unsuspecting individuals. A link or website URL where scammers will ask for your personal and banking information is usually attached to the messages.

03

Vishing: Vishing gains access to your personal information, but this method uses a phone call or voicemail to prompt users to expose private information.

AI-GENERATED DEEPFAKES

Cheapfakes or Shallowfakes are conventionally created altered media

Deepfakes use AI to synthetically create hyper-realistic videos, images, or audio by manipulating content.

Misuse includes impersonating people, spreading misinformation, or conducting fraud.

Scams include (e.g., deepfake videos of CEOs asking for financial transfers) or reputation attacks (e.g., compromising videos).



The New Threats On Social Media

- **Misinformation**

- **Digital arrests**

- **Deepfakes**

- **Voice Cloning**

- **Website Spoofing**



Policies Governing CyberSpace

Telecommunication Bill, 2022

Digital Personal Data Protection Bill, 2022

Intermediary Guidelines, 2021, 2022, 2023

- Social Media Rules
- Online Gaming Rules
- Digital Media Ethics
- Fact-checking Body

Draft Cybersecurity Strategy

Legislative Responses



Digital Personal Data Protection Act, 2023

Enacted to safeguard personal data, this act emphasizes user consent and mandates stringent data handling practices.



Information Technology Rules, 2021

These rules outline the responsibilities of intermediaries and digital media, aiming to curb the spread of harmful content online.



Broadcasting Services (Regulation) Bill, 2023

A proposed law aiming to overhaul the regulatory framework for broadcasting services in India, encompassing a wider range of platforms and technologies.

Cyber Safety Measures



To ensure cyber safety, it is essential to adopt preventive measures. Here are some key steps to safeguard yourself and others in the online world



Strong Passwords: Use complex and unique passwords for all your online accounts to prevent unauthorized access.



Update Software: Regularly update your devices, applications, and antivirus software to patch vulnerabilities.



Secure Wi-Fi: Protect your home Wi-Fi network with a strong password and encryption to prevent unauthorized access.



Think Before You Click: Be cautious while clicking on links, downloading files, or opening attachments, as they may contain malware or phishing attempts.



Privacy Settings: Review and adjust privacy settings on social media platforms and other online services to control the information you share.

Cyber Safety Measures



Multi Factor Authentication: Use multi factor authentication setting in all your devices and applications, this will be immensely helpful in safeguarding your accounts and data.



Active reporting: Netizens should practice active reporting of illicit/fraud/impersonating content, accounts, and pages.



Avoid strangers: Interact with your friends or people you know in real life, avoid interacting with strangers on social media and gaming platforms.



Authentic Apps: Always download authentic apps from trusted app stores, avoid using APK version of apps for convenience.



Antivirus: Use antivirus and anti trojan softwares for all your devices and maintain a close look.

How to Secure your MOBILE PHONES AND TABLETS



Security Lock

Use a number code, pattern lock, fingerprint or Face ID to lock a device when not in use.



Encryption

Encrypt the entire device or just the sensitive data



Remote Wipe

In case the phone stolen or lost, Remote wipe the device



Backup Data

Regularly backup your data



Applications

Do not install anything from an unknown source and research in depth before installing any applications



Messages

Beware of Social Engineering scams, Fake offers, phishing and smishing in particular. Such messages gain access to your personal and financial informations



No Rooting

Avoid Jailbreaking or rooting your device. It often opens your device to backdoors and malware



Update System

Keep your system and applications up to date. An update provides patches for the vulnerabilities. Enable Automatic update Feature



Mobile Internet Security

Firewall and Antivirus is a must for your digital device to be prepared for any potential cyber attack



Switch off Wifi, Bluetooth and NFC

Turn off when not in use. Use VPN when connecting to a Public WIFI network

“INFUSING CYBERPEACE IN CYBERSPACE”

THANK YOU

www.cyberpeace.org secretariat@cyberpeace.net



New Delhi, India



San Francisco, USA



Nairobi,
Kenya



/cyberpeacefoundation



/cyberpeacengo



/cyberpeacefoundation