

The Risks of Oversharing on Social Media

Protecting your digital identity in an interconnected world



What Is



Too Much Personal Info

Disclosing sensitive details online that should remain private



Intimate Relationship Details

Posting private moments and personal conflicts publicly



Daily Routine Updates

Frequent posts revealing patterns and predictable schedules



Permanent Digital Trail

Creating content that's nearly impossible to completely erase



Why Do People Overshare?

Social Connection

- 94% share to entertain or bring value to others
- 78% want to grow and nourish relationships

Psychological Drivers

- Brain reward centres activate with each share
- Anxiety and insecurities fuel oversharing behaviours



📌 **Harvard study: Sharing triggers pleasure responses in the brain, similar to rewards**

The Scale of Sharing Today

Our digital footprints grow exponentially with every post

55M

**Facebook
Updates**

Status updates
shared daily
worldwide

60M

**Instagram
Photos**

Images posted
every single
day

500M

Twitter Posts

Tweets sent
daily across the
platform



Privacy Compromised: Location Sharing Risks

Geotagging Dangers

Reveals your exact location to strangers and potential threats

Tracking Your Movements

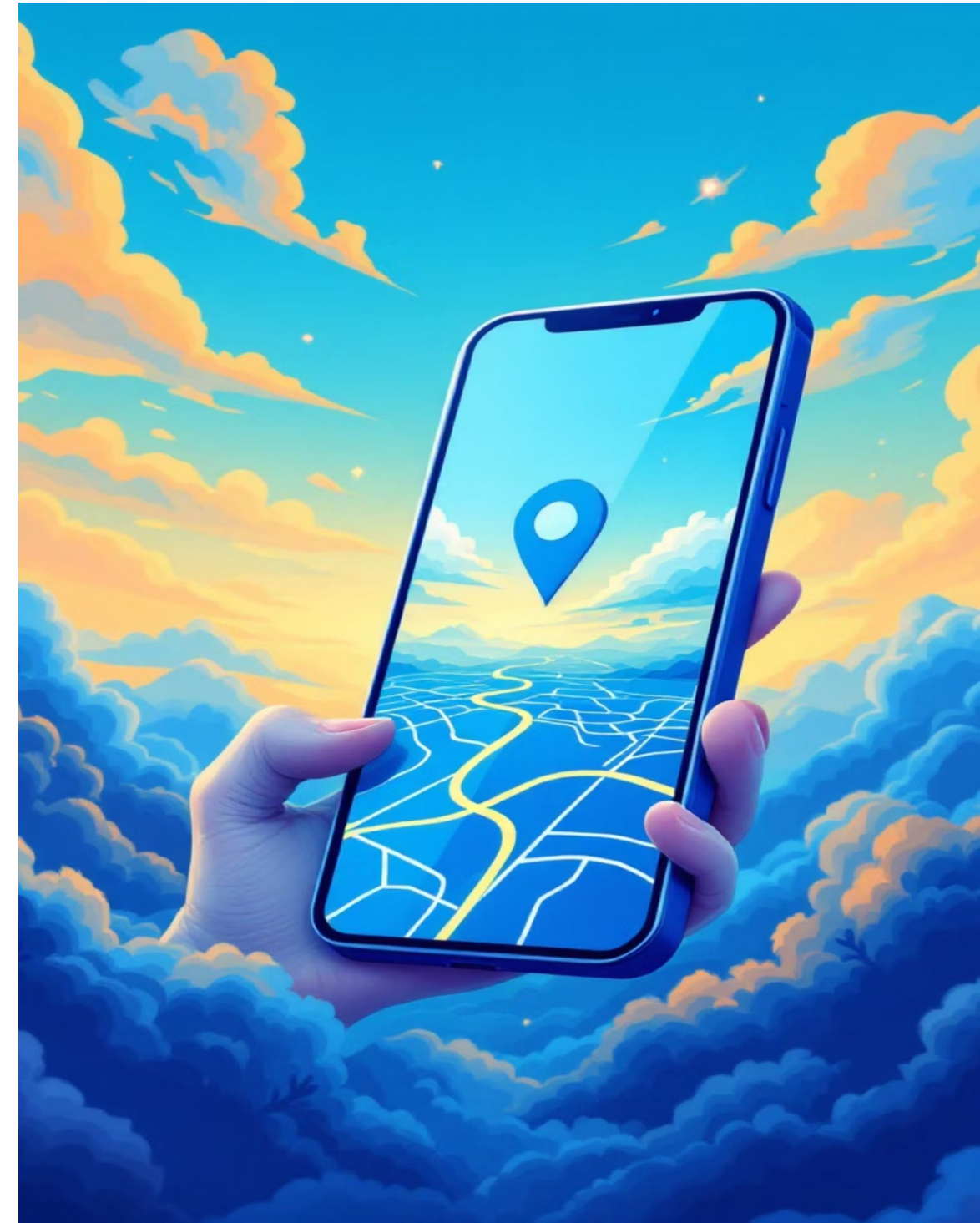
Hackers monitor patterns to plan break-ins when you're away

Disable Location Features

Turn off location sharing and photo geotags immediately

Home Security Risk

Oversharing whereabouts signals when your home is empty



Personal Info: A Hacker's Goldmine



Password Clues Everywhere

Birthdays, pet names, favourite teams crack security questions



Identity Theft Gateway

Cybercriminals exploit shared details for phishing scams



Security Questions Exposed

Avoid posting answers to common account recovery prompts



Strong Privacy Settings

Share only necessary information with trusted connections



Cyberbullying, Cyberstalking & Reputation Damage

Attracting Stalkers

Oversharing enables cyberstalkers to track your activities and patterns

Professional Image Harm

Public rants or personal drama posts damage your career prospects

Employer Screening

Hiring managers increasingly review social media before making offers

Lasting Consequences

One careless post can lead to job loss or social isolation



Identity Theft: Easier Than You Think

Data Collection

Thieves combine shared details from multiple posts and platforms

1

Fraudulent Activity

Loans, credit cards, and accounts opened in your name

3

Impersonation

Criminals use gathered info to assume your identity convincingly

2

Financial Devastation

Extortion, theft, and damaged credit scores follow

4

Use privacy controls and think twice before posting personal data

How to Avoid Oversharing

Make Profiles Private

Limit audience access and control who sees your content

Think Before Posting

Would you say it face-to-face? Apply the same filter online

Curate Your Content

Avoid posting risky or potentially embarrassing material

Update Security Regularly

Use strong passwords and review privacy settings frequently



Final Thought: Share Smart, Stay Safe

Connection vs. Risk

Social media connects us, but oversharing puts us at risk

Control Your Share

Protect privacy by controlling what and how much you post

Permanence Matters

Once online, content can be permanent and widely spread

Think before you post

Your digital safety depends on it



Role of Cyber First Responder

Be a Volunteer in the Cyberspace,
Be a First Responder to Cyber threats

CYBERPEACE CORPS

World's largest community of cybersecurity patrons!



CROWDSOURCING

Skills and knowledge of volunteers, response to information and incidents, training and awareness sustainability.



TRAININGS

Cyber security training through events and inclusion with curriculum, Training outreach by volunteers in civil society



CYBERPEACE CLUBS

Association of students and teachers in Schools and Colleges - opportunity for learning and participation



NETWORK

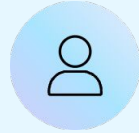
An active volunteer and digitally aware citizen network interacts with government, law enforcement and private industry



COMPETITIONS

Local and national events - Hackathons, Talent identification, Art competitions, Qui, CTF, Public speaking and more

What is a Cyber First Responder?



Trained Community Champion

Individual or institutional representative equipped with knowledge and tools



First Line of Defense

Identifies and responds to emerging cyber threats in real-time

Threat Landscape

- AI-enabled attacks and automation
- Sophisticated fraud schemes
- Misinformation campaigns
- Deepfakes and identity theft

Acts before or alongside law enforcement

Key Responsibilities: Detection & Identification

Early Warning Monitoring

Actively watch for unusual patterns and suspicious activity within the community

Threat Identification

Recognize phishing attempts, account takeovers, and sophisticated digital scams

AI Fraud Detection

Spot AI-driven fraud tactics including deepfake content and automated attacks



Key Responsibilities: Response & Support



Immediate Victim Assistance

Provide clear guidance on emergency safety steps and protective measures



Evidence Preservation

Help victims secure accounts, document incidents, and preserve digital evidence



Professional Referrals

Connect victims to national helpline **1930** and local cyber cells



Case Escalation

Identify serious threats requiring immediate law enforcement intervention

Awareness & Education: Prevention Through Knowledge



Interactive Workshops

Hands-on cyber safety training sessions for all age groups and literacy levels

Cultural Engagement

Competitions, and creative campaigns that resonate locally

Practical Education

Teaching password security, safe browsing, privacy protection, and scam recognition

Digital Hygiene Culture

Building long-term awareness and safe online habits across communities



Cyber First Responder (CFR)

A comprehensive capacity-building program designed to equip institutions and individuals with the skills, knowledge, and resources to respond swiftly and effectively to cyber threats

Mission

Create skilled responders who can recognize early signs of attacks (like phishing, fraud, misinformation, deepfakes), guide victims, and support formal agencies in protecting people and systems.

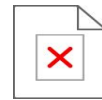
Vision

Vision: A broad grassroots network where schools, colleges, offices, and local groups all have people capable of acting as first responders, making cyberspace safer and more resilient for everyone.

Who Can Join CyberPeace Corps?

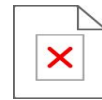


An inclusive initiative for diverse professionals.



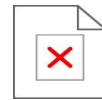
Students

Young learners eager to develop cybersecurity skills and contribute to digital safety



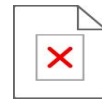
Educators

Teachers and trainers who can integrate cyber awareness into educational programs



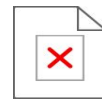
Entrepreneurs

Business leaders and startup founders building secure digital ecosystems



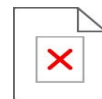
Creative Artists

Designers and content creators producing engaging awareness campaigns



Coders/Developers

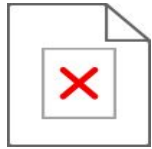
Software developers and tech professionals building security tools and solutions



Professionals (Any Field)

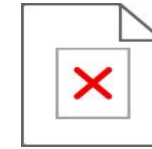
Experts from any industry who want to contribute their skills to cybersecurity initiatives

Target Stakeholders: Building a Network



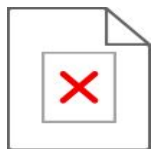
Librarians & Educators

Trusted community figures who serve as knowledge gatekeepers and can reach diverse populations daily



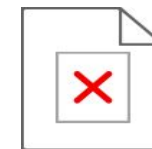
Youth & Students

Digital natives who can become peer educators and drive grassroots awareness among their networks



Law Enforcement

Officers who benefit from community support in early detection and faster case documentation



Institutional Staff

Representatives from NGOs, schools, and local organizations who anchor community programs

Key Program Features

AI Threat Focus

Specialized training on emerging threats:

- Deepfake detection techniques
- Automated phishing recognition
- Misinformation source verification
- AI-generated content identification

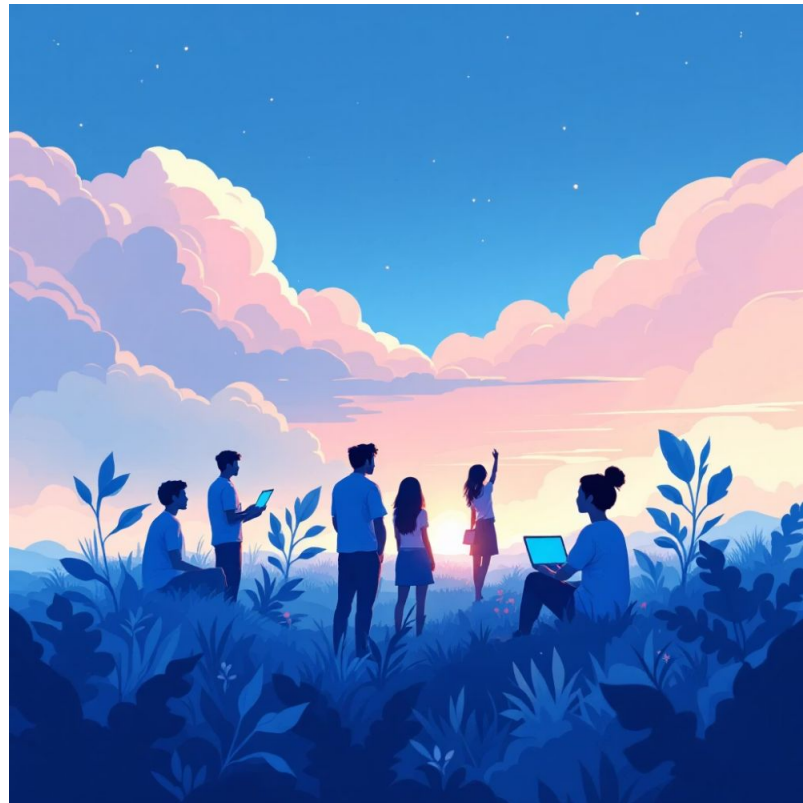
Community-Based Approach

Inclusive, grassroots methodology:

- Culturally relevant training materials
- Local language support
- Accessible to all literacy levels
- Peer-to-peer learning models



Role in Broader Ecosystem



CyberPeace Corps Integration

Part of national volunteer network mobilizing citizen responders

Community Ambassadors

Local volunteers acting as trusted digital safety advocates

1

2

3

4

CyberPeace Yatra Connection

Linked to nationwide awareness journey reaching remote communities

Ground-Level Impact

Combating online harassment, cybercrime, and digital exploitation across rural and urban India

National Impact & Goals



Strengthen Cyber Helplines

Enhance capacity and response times of national helpline infrastructure nationwide



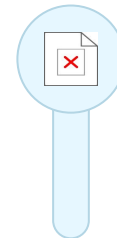
Improve Fraud Detection

Build sophisticated early-warning systems through community intelligence networks



Policy Intelligence

Feed ground-level insights to national policymakers for evidence-based cybersecurity strategies



India AI Impact Summit

Contribute learnings and case studies to shape India's AI safety and governance frameworks

Together, we're building a safer digital India—one community at a time