Quest Journals
Journal of Education, Arts, Law and Multidisplinary
Volume 15 ~ Issue 6 (Nov. – Dec. 2025) pp: 79-82
ISSN(Online): 2347-2895
www.questjournals.org

Research Paper

HONEY TRAP VIA SOCIAL MEDIA
A Legal and Cybersecurity Perspective

Shailej Tiwari
Asst. Professor Department Law Department
College: Katni Arts & Commerce College
(Autonomous) Katni (M.P.)

Abstract

With immense growth in digital connectivity, social media has emerged as a platform for both communication and cyber exploitation. Honey-trap schemes—where offenders use romantic or sexual manipulation to extract or extort sensitive information—have risen significantly in India. This paper examines the concept of honey trapping, techniques used by cyber criminals, psychological vulnerabilities exploited, legal framework under Information Technology Act, 2000 and newly enacted criminal laws including Bharatiya Nyaya Sanhita (BNS), Bharatiya Sakshya Adhiniyam (BSA), and Bharatiya Nagarik Suraksha Sanhita (BNSS). It also highlights enforcement challenges, major case references and preventive measures to protect society from these evolving digital threats as a new concern for upcoming generations and targeting officers of the Government resulting a major threat for national security.

I. Introduction

Social media platforms such as Facebook, Instagram, WhatsApp, Telegram, Snapchat etc. and dating apps have increased human interaction with unknown people. However, the ease of connectivity has also increased exposure to cyber-crimes. Among these, honey trap operations have become a major threat in India. Traditionally associated with intelligence agencies for espionage, honey trapping now involves ordinary cyber criminals who persuade individuals into romantic or sexual exchange and later exploit their trust for monetary or illegal demands, and in case of government officials they demand for the information and secrets of the government.

These crimes cause severe emotional, financial and reputational damage and often go unreported due to social stigma and family prestige. This research aims to analyse honey trap schemes from legal, psychological and social cybersecurity and personal damage perspective.

II. Concept and meaning of Honey Trap

A honey trap refers to intentional manipulation through seduction or emotional bonding by persuading individuals to fulfil their desires to gain access to confidential or compromising information. In social- media based honey traps, fake identities are used to befriend victims, earn trust, and then threaten them by exposing their intimate content or personal secrets.

Forms of Honey Trap

1) Sextortion based: At first they gain trust and record your pictures and videos and then threaten to post this intimate explicit content.
2) Financial Fraud: Extracting money through blackmailing or emotional manipulation.
3) Espionage or Information Extortion: This form of honey trap targets government officials or corporate employees to leak secrets of the government or organisation.
4) Forced illegal activities: They force the victim to get involved into criminal activities like human trafficking, drugs, or escort services.

III. Causes and Contributing Factors

1. Emotional vulnerability
→ Loneliness and desire for companion
→ Vanity and ego

→ Fear of public exposure

2. Lack of cyber awareness

→ Users unaware of digital safety
→ Anonymity and fake profiles
→ Ease of communication

3. Perpetrator motivations and objectives

→ Espionage (national or corporate)
→ Political manipulation
→ Notions of honor and masculinity
→ Stigma and victim blaming

4. Misplaced trust in strangers – acceptance of unknown friend requests and talking to unknown persons to fulfil desires.
5. Criminals hide their identity using AI and other tools very easily.
6. Sometimes greed and material temptation – offers of gifts, money, loans, trips etc. Young adults, government staff, businessmen and the retired elderly are common targets.

IV. Techniques Used in Honey traps

Cyber criminals follow a crafted approach:

1. Identity Fabrication → Fake online personas:

Fake profile with stolen or Al-generated photos are created.

2. Trust building or Emotional grooming:

Regular chats, compliments and promises to build trust and always hitting the emotionally weak point and acting as a supporter.

3. Shifting Communication platforms: Initially contact on social media public platforms like Facebook, Instagram and request to quickly move to private messaging apps like WhatsApp or Telegram for more intimate talk.

4. Content extraction:

Victims are offered for nude video calls, live nude shows on video calls, sharing explicit pictures or bank details, revealing professional information and government secrets.

5. Coercive Exploitation:

Then they start to threat you like:
"Pay or your video will go viral"
"I will upload this on social media or send it to your family".

V. Impact on Victims

1. Psychological depression, anxiety, trauma, these led to suicidal tendencies. 2 Money extortion causing major financial loss.
3. Fear of losing public reputation and social humiliation.
4. Hesitation to file complaint due to legal procedure and court proceedings.
5. Account hacking and identity theft, lack of cybersecurity.

Victim blaming led to discourage in reporting, it worsens the suffering, and gives strength to offenders.

VI. Legal Framework in India

A. Information Technology, Act, 2000

Section Penalize:-

1. Sec. 66 C - Identity theft -

using another person's identity/profile/data.

2. Sec. 66 D - Cheating by impersonation online.
3. Sec. 67 and 67 A - Publishing / transmitting obscene or sexually explicit content.
4. Sec. 69 A - Blocking harmful / extortion related content.

B. Bharatiya Nyaya Sanhita (BNS), 2023

Sec. 316 - Extortion and threats causing delivery of property. Sec. 318 - Cheating and dishonestly inducing property transfer. Sec. 351 - Criminal intimidation to cause harm to reputation Sec. 357 - Defamation harming social image.

Sec. 63 - Sale or distribution of obscene sexual content.

See 73 and 74→ Voyeurism - Capturing private acts, sharing images. Sec. 86 - Insulting the modesty of a women.

Where minors are involved :- POCSO Act ensures stringent punishment.

C. Bharatiya Nagrik Suraksha Sanhita. BNSS (2023).

BNSS governs complaints, arrests, investigation and trials such as:
-Filing FIR under Sec. 173.
-Electronic evidence based arrest warrants.
-Faster digital investigation mechanisms.
-Cyber police stations operate under BNSS provisions.

D. Bharatiya Sakshya Adhiniyam (BSA) 2023

1. Sec. 57 - It recognizes electronic evidence as primary evidence.
2. Expanded definition of "document" in Section 2(1)(d). Includes electronic and digital records.
3. Sec 63 - Introduces format format for the certificate needed to present electronic evidence in Court.
4. Sec. 58 - Expands the scope for secondary evidence of electronic records. Thus, law recognizes digital footprints as strong evidence.

VII. Case studies in India

1 Madhya Pradesh Honey Trap Scandal (2019):
A network blackmailed influential leaders using secretly recorded intimate content-revealed deep organized exploitation.[1]
2. Sextortion Rackets in Delhi-NCR (2022-2023).
Nigerian and local gangs used Instagram/WhatsApp video calls to trap businessman and youths: hundreds of victims reported.[2]
3. Mumbai Honey Trap Arrests (2023):
Young women created fake profiles, trapped men's, and demanded ransom threatening the leak content.[3]
4. Kirti Patel Sextortion Case:
Social media influencer Kirti Patel (aka Kirti Adalja) was arrested for allegedly honey trapping a builder and extorting Rs. 2 crore. [4]
5. Archona Nag Sextortion Racket:

Archana Nag was allegedly involved in a large sextortion / honey trap ring in Odisha, blackmailing rich people and politicians.[5]

6. Rajasthan minister Honey Trap :
Three were arrested for allegedly trying to Honey Trap Rajasthan Minister Ramlal Jat.[6]

VIII. Challenges in Enforcement.

1. Perpetrators operate across countries having a transnational nature.
2. Fake digital identity VPNs, spoofing hinder tracing.
3. Victims fear shame and harassment led to low reporting.
4. Law enforcement lacks equal training due to rapid change in technologies.
5. Social media companies require long legal procedures which hurdles fast data access.

[1] Hindustan Times (News Article): Abraham, "Media, politics, sex: Untangling a scandal that rocked Madhya Pradesh", Hindustan Times, Dec. 26, 2019,

[2] Times of India (News Article): "Sextortion cases on rise, be careful on social media", Times of India, Feb. 10, 2022,

[3] India Today (News Article/Analysis): Singh, "Honeytraps and high treason: The faces behind India's spy scandals", India Today, May 20, 2025

[4] The Economic Times (News Article): "Kirti Patel sextortion case: Influencer with over 10 lakh followers, arrested in Gujarat for honey-trapping builder", The Economic Times, June 19, 2025

IX. Preventive measures

Individual level

~ Avoid accepting friend requests from unknown profiles.

~ Do not share intimate visuals online.

~ Verify identity through real time audio/video call.

~ Use strong passwords and two-factor authentication.

~ Report immediately to cybercrime.gov.in #Goverment or Institutional level
~Compulsory cyber awareness in colleges and workplaces.
~Strengthening cyber forensics and cyber police training.
~Quick takedown and permanent deletion of threating content.
~Policy to label suspicious and unidentified profiles.
~Law and cybersecurity infrastructure must evolve simultaneously. #Platform Responsibility
~AI based fake account detection
~Faster response to sextortion reports.
~Transparent cooperation with authorities.

X. Recommendations

~Specific legislation should be drafted on Honey-trapping and sextortion.
~Such incidents must be treated as cyber gender-based violence.
~A 24x7 cyber counselling and victim-support system should be established.
~Increase in international cooperation for data sharing and easy access.
~Public campaigns to reduce stigma and encourage reporting of the incidents.
~Legal, Social and digital empowerment are needed for effective solutions.
~Improved cyber policing and digital literacy.
~A victim centric approach should be. adopted in these honey- trap cases.

XI. Conclusion

Honey trapping via social media is emerging as a severe cyber threat and a new social evil in India. The anonymity and reach of technology empower trust for unlawful gain. Though the IT Act, BNS, BNSS, and BSA provide legal remedies to victims, But the hesitation and fear plus enforcement gaps weaken justice delivery.

A combined response is essential and only then society can ensure a safe digital environment where relationships built online do not become traps of exploitation.

Bibliography

Books & Journals

[1]. Aparna Sharma ;Cyber Crime and Law in India. LexisNexis, 2022.
[2]. Ranbir Singh; Law Relating to Information Technology. Universal Law Publishing, 2023.
[3]. S. Jain; "Digital Deception and Emotional Exploitation: A Study of Honey Trap Crimes." Indian Law Review, 2022.
[4]. *Nir Kshetri; "Emerging Threats in Indian Cyberspace." Journal of Cybersecurity Studies, 2021.

Statutes

[5]. Information Technology Act, 2000.
[6]. Bharatiya Nyaya Sanhita, 2023.
[7]. Bharatiya Nagrik Suraksha Sanhita, 2023.
[8]. Bharatiya Sakshya Adhiniyam, 2023.
[9]. Protection of Children from Sexual Offences Act, 2012.

Government & Digital Sources

[10]. NCRB. Crime in India Report — Cyber Crime Sections, 2020–2023.
[11]. CERT-In. Advisories on Sextortion and Online Blackmail.
[12]. Press Information Bureau (PIB), Government of India. Cyber Safety Bulletins, 2023.

[5] Hindustan Times (News Article): Mohanty, "Odisha blackmailing case: Archana Nag to be released from prison after...", Hindustan Times, Dec. 4, 2023,

[6] India Today (News Article on separate, related case): "Rajasthan man arrested for spying for Pakistan, was honey-trapped by...", India Today, Oct. 11, 2025