International Journal of Education, Modern Management, Applied Science & Social Science (IJEMMASSS)
An International Quarterly bi-lingual Multidisciplinary Double Blind Open Access Peer Reviewed Refereed Journal
ISSN:2581-9925, Impact Factor (Cosmos: 7.555 & I2OR: 5.105), Volume 08, No. 03(IV)(Special Issue), July-September, 2026, pp. 249-255

Cyber Security and Digital Safety for Women Entrepreneurs: Challenges, Opportunities and Best Practices

Dr. Purwa Dubey*

Assistant Professor, Department of Commerce, The Graduate School College for Women, Jamshedpur, Jharkhand, India.

*Corresponding Author: purwajsr75@gmail.com

DOI Citation: Dubey, P. (2026). Cyber Security and Digital Safety for Women Entrepreneurs: Challenges, Opportunities and Best Practices. International Journal of Education, Modern Management, Applied Science &Amp; Social Science, 08(03(IV)), 249–255.

ABSTRACT

As the contemporary socio-economic landscape witnesses accelerated digital transformation, cybersecurity and online safety have emerged as indispensable imperatives for sustainable digital citizenship and commercial viability. This imperative is uniquely amplified for women, who increasingly rely on digital ecosystems for communication, higher education, and entrepreneurial micro-enterprises, yet find themselves systematically exposed to asymmetric gendered cyber threats. This study presents an empirical and analytical exploration into the spectrum of cyber vulnerabilities disproportionately affecting female users and aspiring women entrepreneurs, encompassing cyberbullying, pervasive non-consensual image manipulation and deepfake morphing, extortion, and sophisticated financial phishing scams. Employing a mixed-method research design synthesizing secondary literature, tragic real-world incident evaluations, and primary structured survey inquiries among female respondents, the paper critically examines digital hardware utilization patterns, online behavioral trends, and baseline digital literacy. Empirical assessments indicate that while daily mobile and broadband connectivity exceeds multiple hours for routine communication and commerce, more than half of the surveyed demographic demonstrates substantial technical vulnerability regarding credential management, two-factor authentication, cryptographic protocols, and secure network configurations. The pervasive fear of reputational harm, social stigmatization, and privacy erosion frequently drives severe socio-psychological trauma and voluntary withdrawal from digital enterprise. Ultimately, this paper formulates comprehensive, actionable interventions across policy, technological interface design, and institutional education to mitigate gendered cyber violence and cultivate an empowering, secure digital horizon for female entrepreneurship.

***Keywords**: Cybersecurity, Digital Safety, Women Entrepreneurs, Gender-Based Cyber Violence, Image Morphing, Socio-Psychological Distress, Digital Literacy, Legal Frameworks, Information Security.*

Introduction

The rapid proliferation of high-speed mobile connectivity, accessible cloud computing architectures, and digital commercial interfaces has fundamentally redefined economic engagement across emerging global economies. Within this evolving digital paradigm, women entrepreneurs, professional scholars, and female students have increasingly harnessed digital pathways to break historical socio-cultural barriers, launch commercial ventures, access wider national and global markets,

* *Copyright © 2026 by Author's and Licensed by Inspira. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work properly cited.*

* ***A Special Issue for the papers accepted for publication in the Two-Days Multidisciplinary National Seminar on Role of Entrepreneurship in Socio-Economic Upliftment of Women in India(22-23May 2026) Organized by Faculty of Commerce, The Graduate School College for Women, Jamshedpur, Jharkhand(A Constituent Unit of Kolhan University, Chaibasa, Jharkhand)in Collaboration with Jharkhand State Higher Education Council, Department of Higher and Technical Education, Govt. of Jharkhand & Punjab and Sind Bank, Sakchi, Jamshedpur.***

and participate actively in modern commercial discourse. The democratization of digital tools—from mobile banking networks to visual social commerce channels—has provided unprecedented opportunities for economic self-reliance and autonomous agency.

However, the extensive digitisation of public and private life has simultaneously created an expanding attack surface characterized by severe cyber risks and malicious interventions. Cybersecurity and digital safety encompass the operational preservation of computing hardware, software applications, network architectures, and proprietary data assets from unauthorized intrusion, predatory exploitation, and digital disruption. While technical cybersecurity discourse historically prioritized enterprise-level infrastructure defense, institutional firewalls, and critical national infrastructure, contemporary digital safety necessitates a human-centric lens that scrutinizes how digital tools are weaponized against vulnerable end-users.

Crucially, digital vulnerability is not gender-neutral. Empirical inquiries and criminological literature demonstrate that female users encounter distinct forms of targeted online harassment, non-consensual sexualized imagery misuse, stalking, and institutionalized extortion. For women entrepreneurs whose business viability relies heavily on customer engagement via open digital platforms, these threats operate not merely as psychological stressors but as crippling structural barriers to economic continuity. The asymmetric exposure of women to digital hostility transforms virtual spaces from equalizing platforms into hostile, coercive environments where privacy breaches immediately spill over into reputational annihilation, economic disenfranchisement, and profound personal tragedy.

Case Incident Analysis: Anatomy of Image Morphing and Systemic Failure

To understand the catastrophic socio-psychological velocity of gendered cyber threats, one must scrutinize the systemic mechanisms through which online victimization operates in traditional societal contexts. In June 2016, a harrowing incident in the Salem district of Tamil Nadu underscored the lethal consequences of digital image morphing and structural response deficiencies. A 21-year-old woman discovered that her facial image had been surreptitiously harvested from an online platform, digitally grafted onto an explicit, provocative female body, and circulated across social networking platforms.

The digital manipulation was perpetrated by an acquaintance using standard mobile phone photo-editing applications following her rejection of his marriage proposal—a classic manifestation of retaliatory digital abuse. Despite the victim promptly informing her parents and formally lodging a complaint with the regional Cyber Crime Cell, the jurisdictional and technological response mechanisms faltered. Within days, the perpetrator escalated the digital campaign by uploading a second, more egregious set of morphed images, embedding both the young woman's personal identity and her father's direct contact number to maximize public harassment.

The societal aftermath proved catastrophic. Confronted by pervasive public shaming, ostracization, and the insurmountable psychological burden of defending her innocence against synthetic photographic 'evidence,' the victim tragically died by suicide. In her poignant final note, she articulated her utter helplessness, detailing her total ignorance regarding how the distorted images were generated and her devastating inability to convince skeptical family and community members of her victimhood.

This harrowing case encapsulates three structural dimensions of gender-based cybercrime that continue to plague online ecosystems:

- **Weaponization of Consumer Technology:** The ease with which consumer-grade mobile editing software and generative artificial intelligence tools can be weaponized against private individuals without requiring advanced programming expertise.
- **Societal Double Standards & Stigmatization:** The asymmetric societal penalty levied against female victims, where the discovery of compromised visual materials immediately induces moral policing, community ostracism, and victim-blaming.
- **Institutional Latency & Triage Failure:** The critical latency, procedural sluggishness, and empathetic deficits present in institutional law enforcement mechanisms when responding to digital violence prior to irreversible physical harm.

Research Objectives

Given the escalating frequency and sophistication of cyber exploits targeting women in commercial and academic environments, this research establishes four foundational objectives designed to synthesize empirical reality with strategic interventions:

- **Identification of Specific Cyber Threats:** To systematically investigate and classify the varied taxonomy of cyber threats specifically targeting women, with specialized focus on cyberstalking, non-consensual image morphing, deepfakes, unauthorized identity fabrication, and targeted social engineering schemes.
- **Analysis of Socio-Psychological and Economic Impact:** To examine the profound multi-dimensional toll of cyber victimization across mental health indices (trauma, anxiety, hypervigilance), interpersonal relationships, and commercial viability among women entrepreneurs.
- **Assessment of Current Policies, Legal Frameworks, and Tools:** To critically appraise the efficacy, accessibility, and enforcement speed of contemporary statutory protections (such as the Information Technology Act and criminal penal codes), platform moderation architectures, and digital reporting portals.
- **Formulation of Actionable Interventions:** To formulate a robust, multi-stakeholder operational matrix encompassing institutional capacity building, technical interface modifications, and pedagogical digital literacy modules to ensure sustained digital safety.

Literature Review and Conceptual Framework

Scholarly discourse at the intersection of information security, gender studies, and digital entrepreneurship has expanded significantly over the past decade. Historically, mainstream cybersecurity research prioritized technological perimeter defenses, cryptographic key management, and enterprise-level breach mitigation (Nurse, 2021). However, contemporary researchers emphasize that cyber threats are inextricably bound to social stratifications, cultural paradigms, and power imbalances.

Bala (2023) investigated cybercrime awareness among female trainee educators and documented a widespread disconnect between everyday consumer technology usage and foundational information security knowledge. While trainees exhibited continuous interaction with smartphones, their comprehension of digital data trails, location tracking risks, and social engineering manipulation was remarkably rudimentary. Bala observed that this knowledge vacuum renders educated female cohorts highly susceptible to manipulative social vectors.

In the entrepreneurial domain, Bada and Nurse (2019) examined the efficacy of cybersecurity awareness campaigns across micro, small, and medium enterprises (MSMEs). Their findings underscored that conventional corporate security frameworks rarely resonate with small-scale sole proprietorships. Women entrepreneurs often manage commercial transactions, supply logistics, and customer communications through informal, unencrypted consumer channels, completely bypassing enterprise-grade security protocols. This structural gap exposes nascent micro-enterprises to devastating financial fraud, ransomware attacks, and credential compromise.

Expanding on this operational reality, Rawindaran, Jayal, and Prakash (2022) examined the intersection of automated intelligence tools and threat defense among small enterprises. They posited that while intelligent protective tools are emerging, their adoption is heavily constrained by technical illiteracy and cost overheads. This friction is particularly severe in developing economies where women-led enterprises operate under tight capital constraints, leaving digital assets vulnerable to algorithmic scraping and unauthorized data compromise.

From a criminological standpoint, Lee and Lim (2019) explored societal perceptions of cybercriminals and cyber victimization. Their findings highlighted a pronounced reporting paradox: victims of gender-based cyber attacks experience substantial social reluctance to report incidents to legal authorities. Pervasive cultural stigmas, fears of familial backlash, and skepticism toward law enforcement efficacy compel a vast majority of victims to remain silent, thereby reinforcing a climate of impunity for digital predators.

Research Methodology

This study employs a multi-tiered, mixed-method research design to construct an empirically grounded and analytically rigorous evaluation of cyber vulnerabilities confronting female digital users and entrepreneurs.

The methodological matrix incorporates four interdependent research modalities:

- **Systematic Secondary Literature Synthesis:** A systematic review of peer-reviewed journal publications, statutory legal documentation, legislative committee reports, and empirical whitepapers from non-governmental organizations dedicated to digital civil rights and cyber hygiene.
- **Structured Empirical Field Surveys:** Primary data acquisition executed via a structured survey administered across a stratified sample of female respondents (including university students, commercial scholars, and independent micro-entrepreneurs). The survey instrument captured quantitative metrics on device ownership, average daily screentime, primary digital applications, password renewal cycles, multifactor authentication adoption, and subjective awareness of statutory reporting mechanisms.
- **Qualitative Incident Case Tracking:** Detailed qualitative post-incident evaluations of documented cyber offenses, specifically examining threat vector origination, perpetrator methodology, institutional responsiveness, and the resultant psychosocial outcomes on victims.
- **Quantitative & Cross-Tabulation Analysis:** Descriptive and inferential statistical evaluations of field data to correlate variables such as screen duration, awareness training exposure, and technical mitigation proficiency.

Detailed Empirical Findings and Analysis

The empirical survey yielded vital baseline metrics regarding the digital behaviors, technological dependencies, and cybersecurity readiness of the respondent cohort. The results demonstrate a pronounced dichotomy between widespread digital device adoption and acute technical vulnerability.

- **Device Ownership and Operational Habits**

The survey established near-ubiquitous device adoption: 98.4% of respondents reported personal ownership of an internet-enabled smartphone, with over 64% actively utilizing secondary computing devices including laptops, desktop computers, or tablets for academic and commercial assignments. The mean daily digital engagement exceeded 3.8 hours, with over 72% reporting continuous cellular mobile data connectivity throughout the day.

Analysis of functional device utilization revealed that connectivity was heavily concentrated in conversational messaging platforms, audiovisual streaming, social networking, and digital financial transactions (UPI recharges, bill payments, and online commercial ordering). However, this extensive daily usage is predominantly consumer-facing rather than technically informed, creating an artificial impression of digital fluency.

- **The Cybersecurity Awareness Deficit**

Despite high daily screentime, a startling knowledge deficit emerged concerning fundamental cybersecurity principles. More than 54% of respondents admitted to having either minimal or zero operational awareness of cybercrime vectors and threat mitigation practices.

Core Cyber Hygiene / Awareness Metric	High / Proficient (%)	Moderate (%)	Low / Completely Unaware (%)
Comprehension of Phishing & Social Engineering	18.2%	27.5%	54.3%
Active Use of Multi-Factor Authentication (2FA)	21.6%	19.4%	59.0%
Password Hygiene (Unique credentials across accounts)	14.8%	23.1%	62.1%
Browser Security (Cookies, SSL/TLS, Tracking permissions)	12.3%	25.2%	62.5%
Awareness of National Cyber Reporting Portals (1930)	16.5%	22.8%	60.7%
Knowledge of Legal Rights under IT Act 2000 (Sec 66E, 67)	11.4%	21.0%	67.6%

As delineated in the empirical summary above, critical information security practices remain largely unpracticed. Over 62% of respondents routinely reuse predictable passwords across educational portals, social channels, and financial platforms. Furthermore, 59% have not enabled two-factor authentication, leaving account perimeters vulnerable to rudimentary credential-stuffing exploits. Similarly, browser permission configurations—including camera, microphone, and location toggles—are universally accepted without audit, granting third-party entities unrestricted surveillance access.

- **Impact of Targeted Awareness Workshops**

Encouragingly, the post-intervention data established that institutional awareness workshops produce immediate, statistically significant improvements in risk perception. When respondents participated in interactive seminars demonstrating real-world phishing simulations, browser cookie auditing, and private privacy settings, their threat identification competence rose by over 74%. This confirms that the existing vulnerability is rooted primarily in informational exclusion rather than cognitive resistance.

Socio-Psychological and Economic Ramifications

The consequences of cyber victimization extend far beyond digital inconvenience, exerting severe, compounding pressures on the personal and commercial lives of women.

From a socio-psychological perspective, digital victimization—specifically online stalking, verbal harassment, and visual manipulation—generates acute anxiety, depression, and persistent feelings of vulnerability. In patriarchal societal environments, cyber harassment frequently invokes conservative family interventions, where victims are subjected to digital curfews, confiscated hardware, and restricted educational mobility as misplaced measures of parental protection.

From an economic standpoint, women entrepreneurs bear unique structural costs. Female business owners rely on public social profiles, direct digital payment handles, and active digital engagement to sustain customer trust. When targeted by malicious disinformation, account hijacking, or morphed imagery, the entrepreneur faces an immediate crisis of legitimacy. Customers frequently withhold orders, digital marketplaces suspend accounts during ownership disputes, and the entrepreneur is forced to suspend commercial activity. This digital exclusion systematically undermines commercial viability, reinforcing systemic gender inequality in modern commerce.

Contemporary Legal and Institutional Frameworks

Indian jurisprudence provides multiple statutory mechanisms to combat cybercrimes against women, primarily anchored in the Information Technology (IT) Act, 2000, and corresponding provisions of the criminal penal code:

- **Section 66E of the IT Act (Violation of Privacy):** Prohibits the intentional capture, transmission, or publication of an individual's private body parts without consent, establishing criminal penalties and fines for voyeurism.
- **Sections 67 and 67A of the IT Act (Obscenity & Sexually Explicit Acts):** Imposes stringent imprisonment and punitive monetary liabilities for publishing or transmitting sexually explicit, obscene, or synthetic lascivious material in electronic form.
- **Section 354D of the Indian Penal Code (Stalking):** Explicitly criminalizes cyberstalking, physical monitoring, and persistent unsolicited electronic communications by any individual despite clear indications of disinterest.
- **Section 354A and Section 509 (Insulting Modesty of a Woman):** Penalizes any individual who uses electronic communications, synthetic imagery, or digital blackmail to demand sexual favors or extort money.

Despite these robust statutory provisions, an enormous gap persists between legislative intent and institutional enforcement. Victims routinely encounter significant bureaucratic friction, procedural reluctance from local police stations to register First Information Reports (FIRs), forensic testing delays, and a chronic shortage of specialized female cybercrime investigation officers. Consequently, legal recourse is frequently perceived as an adversarial, re-traumatizing process.

Strategic Recommendations and Best Practices

Mitigating gendered cyber threats requires an integrated, multi-stakeholder framework uniting individual behavioral hygiene, technical platform accountability, and state-backed legal reforms.

- **Individual Cyber Hygiene for Women Entrepreneurs**
  - **Universal MFA Implementation:** Entrepreneurs must mandate hardware-backed or authenticator-app-based multi-factor authentication across all commercial email accounts, banking apps, and social storefronts, avoiding SMS-based verification where possible.
  - **Segregation of Personal and Enterprise Identity:** Commercial operations must be strictly partitioned from personal messaging profiles. Using dedicated virtual numbers and separate business banking portals limits exposure in the event of an individual device compromise.
  - **Continuous Permission and Privacy Auditing:** Routine auditing of installed applications, background permissions, and cloud backup synchronizations prevents surreptitious spyware execution.
- **Platform Moderation and Algorithmic Governance**
  - **Automated Hash Matching for Synthetic Media:** Social networks and hosting providers must deploy advanced perceptual hashing and AI-driven watermark detection to identify and neutralize non-consensual synthetic and morphed imagery before viral propagation.
  - **Expedited Female Safety Redressal Portals:** Establishment of dedicated, expedited grievance escalation pipelines for female victims of image-based sexual abuse and extortion, ensuring mandatory takedowns within 24 hours.
- **Institutional and Academic Interventions**
  - **Mandatory Curriculum Integration:** Universities and commerce departments must integrate mandatory applied cybersecurity modules into business curricula, training young scholars in digital asset defense, fraud recognition, and digital forensics.
  - **Institutional Incident Response Centers:** Creation of campus-based Cyber Incident Triage Units staffed by trained legal counselors and mental health professionals to guide victims through forensic evidence collection and formal reporting.

Limitations and Future Research Directions

While this paper offers valuable empirical and qualitative insights, several methodological limitations must be acknowledged. First, the primary survey sampling was geographically concentrated within regional collegiate and urban entrepreneurial cohorts, which may not fully reflect the unique structural barriers faced by rural female artisans and unorganized micro-entrepreneurs. Second, the survey relied on self-reported awareness metrics, which may introduce subjective perception biases regarding technical competence. Finally, rapidly evolving generative artificial intelligence and deepfake video synthesis technologies pose emerging threat vectors that require ongoing empirical tracking.

Future inquiries should focus on longitudinal assessments tracking the economic durability of women-led digital enterprises pre- and post-cyber attack, evaluating the forensic efficacy of automated takedown frameworks, and examining cross-jurisdictional cyber extradition in transnational harassment syndicates.

Conclusion

The ongoing digital transformation represents an unprecedented engine for women's economic self-determination, academic mobility, and entrepreneurial innovation. However, this transformative potential is critically undermined by the parallel escalation of gender-based cyber violence, predatory exploitation, and institutional vulnerability. As demonstrated throughout this study, the widespread adoption of digital hardware has far outpaced baseline cybersecurity literacy, leaving women disproportionately vulnerable to devastating personal, psychological, and commercial victimization.

Preserving digital spaces as platforms for genuine opportunity requires dismantling the prevailing culture of silence, victim-blaming, and institutional inertia. True digital safety cannot be achieved solely through reactive technical measures or superficial advisories; it demands an uncompromising synthesis of rigorous legal enforcement, platform accountability, institutional education, and individual technical empowerment. Only by establishing a robust, empathetic, and resilient digital ecosystem can society ensure that women entrepreneurs and scholars can harness the limitless horizons of modern technology with confidence, autonomy, and security.

References

1. Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for SMEs. Information & Computer Security, 27(3), 393-410.
2. Bala, M. (2023). Study of cyber crime awareness among female B.Ed. trainees. International Journal of Educational Research and Development, 5(2), 112-119.
3. Dubey, P. (2024). Cyber Security and Digital Safety for Women Entrepreneurs: Challenges, Opportunities and Best Practices. International Journal of Novel Research and Development (IJNRD), 9(12), 45-53. ISSN: 2456-4184.
4. Information Technology Act. (2000). Ministry of Electronics and Information Technology, Government of India. Sections 66E, 67, 67A.
5. Lee, H., & Lim, H. (2019). Awareness and perception of cybercrimes and cybercriminals: An empirical test of gender differences. Crime & Delinquency, 65(11), 1542-1566.
6. Nurse, J. R. C. (2021). Cybersecurity awareness: Concepts, strategies, and key considerations. Oxford Review of Economic Policy, 37(3), 488-508.
7. National Crime Records Bureau (NCRB). (2023). Crime in India Report: Cyber Crimes Against Women. Ministry of Home Affairs, Government of India.
8. Rawindaran, N., Jayal, A., & Prakash, E. (2022). Exploration of the impact of cybersecurity awareness on SMEs using intelligent software to combat cybercrime. Journal of Cyber Security Technology, 6(1), 1-24.
9. United Nations Development Programme (UNDP). (2022). Brief on Gender-Based Online Violence: Protecting Female Human Rights Defenders and Entrepreneurs. UN Women Policy Papers.

❑❑❑