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. 153-155

Cyber Security and Digital Safety for Women Entrepreneurs

Dr. Savita Mishra[1*] | Dr. Jyoti Kumari[2]

[1]Assistant Professor, Department of Mathematics, The Graduate School College for Women, Jamshedpur, Kolhan University, Chaibasa, Jharkhand, India.
[2]Assistant Professor, Department of Philosophy, The Graduate School College for Women, Jamshedpur, Kolhan University, Chaibasa, Jharkhand, India.

[*]Corresponding Author: savitamishrajsr@gmail. com

DOI Citation: Mishra, S., & Kumari, J. (2026). Cyber Security and Digital Safety for Women Entrepreneurs. International Journal of Education, Modern Management, Applied Science &Amp; Social Science, 08(03(IV)), 153–155. https://doi.org/10.62823/ijemmasss/8.3(iv).9601

ABSTRACT

Women can't run a modern business without solid digital protection. Women-led startups are building smarter security solutions. Workplaces today are flexible, and so are the risks. Instead of overwhelming businesses with complex systems, they focus on practical tools anyone can use. Each digital interaction—an email, a file, a login—presents inherent risks, but also a chance to cultivate confidence. Women business owners are breaking old molds. They combine smart new ideas with heartfelt concern. What these leaders do makes it plain: cybersecurity isn't just a technical challenge; it fundamentally addresses the human element. We will discuss and summarise solution that maps with the priorities of many women-led cybersecurity ventures—simple, secure, and smart. Female entrepreneurs encourage companies to view security as a team effort. What makes many female entrepreneurs stand out is their bigger picture view. For them, digital safety is tied to social responsibility. Protecting vulnerable groups online, making safe tools affordable, and raising awareness around digital rights—these are priorities that go beyond profit.

***Keywords**: Cyber Crime, Cyber Security, Women Security, Basic Rights, Digital Protection, Women Entrepreneurs.*

Introduction

In today's connected[9] world, online safety is no longer optional—it's essential. The mission is to empower women with safer digital environments. Digital platforms[2] have empowered entrepreneurs in unprecedented ways, opening doors to education, career growth, and entrepreneurship. However, this digital progress[2] must be supported by strong cyber security[9] practices. Women are often targeted through social engineering, scams, harassment, and digital surveillance [2,3]. Through cyber awareness initiatives, secure practices, and innovative physical data security tools such as USB Port Locks and Blockers, the company helps protect both personal and professional data from unauthorized access. Digital safety is not just about technology—it is about protecting privacy[2], confidence, and independence in an increasingly connected world. Female entrepreneurs understand that lasting digital safety isn't built in isolation. They often create partnerships with other companies, industry groups, and even government agencies to share resources and knowledge. These collaborations mean better protection against fast-changing cyber threats. Female entrepreneurs are showing us that digital safety[1,2,7,8] is more than technical protection—it's a mindset. By making security inclusive, ethical, and

[*] *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.***

adaptable, they are building workplaces that people trust. Their leadership proves that safety and innovation can go hand in hand. Women working in offices, remote environments, educational institutions, or public workplaces often use shared computers or systems. In such situations, physical port security becomes extremely important. Physical data security tools help by:Securing shared office computers; Protecting confidential work files; Preventing unauthorized data copying; Blocking malware from infected USB drives; Ensuring safe device usage in public environments. By securing the physical access points of devices, women entrepreneurs can work with bigger confidence and peace of mind. Awareness is the most powerful tools in cyber security[5,6,7]. Encouraging the use of secure devices; Providing access to reliable security tools; When women Protecting confidential work files are equipped with knowledge and protective technology, they are better prepared to navigate the digital world safely. Building a Safer Digital Environment is need of the hour.

Cyber security is not just the responsibility of IT professionals—it is a shared responsibility for individuals, organizations, and society. As more women become leaders, entrepreneurs, professionals, and digital creators, ensuring their online safety becomes even more important. Technology companies are contributing to this mission by developing innovative solutions that focus on protecting devices and preventing data breaches. By combining cyber awareness, safe digital habits, and physical data security tools, women entrepreneurs can confidently participate in the digital economy without fear of cyber threats.

Cyber Security and Digital Safety for Women Entrepreneurs

Interconnectedness through the digital space in this day and age has opened up various opportunities; however, it has also left space for crimes to be fostered and the subsequent need for regulation. Digital spaces pose threats to women and girls in the same vein as the physical world, in that they are disproportionate targets of violence. It is no secret that today women are at the helm across different industries. Digital platforms have gradually transformed into predating grounds. Women entrepreneurs are subjected to different kinds of cyberattacks, such as doxxing, sextortion, cyberstalking, and IP thefts. Further, their social image is branded accordingly. The laws might be well-equipped, but there is a dire need to create IP awareness alongside accessible legal frameworks to create an inclusive digital economy. Women Entrepreneurs experience unique digital threats—from identity theft and cyberstalking to phishing and fake job scams. Knowing how to recognize and prevent these attacks is the first step to staying safe online. The swift proliferation of digital technologies is generating novel prospects for growth and advancement, particularly in developing nations. However, the advantages of digitalization are not universal, and women worldwide continue to encounter numerous barriers to thriving in the digital economy, including gender bias, diminished involvement in decision-making, insufficient digital competencies, lack of confidence, and inequitable access to funding, among others. Examples of risks ; Impersonation or doxxing Harassment and cyberbullying; Malicious links in social media DMs; Job and scholarship phishing scams. According to the United Nations Population Fund (UNFPA), technology is increasingly being weaponized to perpetrate gender-based violence. Online harassment, financial fraud, deepfake abuse, and cyberstalking are persistent dangers that women around the world routinely encounter. However, Technology-Facilitated Gender-Based Violence (TFGBV) has real-life consequences. Cyber violence[10] not only threatens safety but also takes a serious toll on women's mental health, leading to low self-esteem, trauma, and emotional distress. As the world becomes increasingly digital, women retreating from online spaces due to cyber threats has far-reaching social, political, and economic consequences. It contributes to social isolation, limits access to education and professional opportunities, and reduces women's economic participation. There is need to equipping women entrepreneurs with essential skills to safeguard their businesses against online threats. The interactive sessions covered key cybersecurity strategies, risk mitigation techniques, and confidence-building in navigating the digital landscape. In today's digital world, women are increasingly using online platforms for education, careers, entrepreneurship, banking, and social networking[3,5]. The internet has opened countless opportunities, allowing women to work remotely, manage businesses, learn new skills, and stay connected globally.

Furthermore, another However, as digital engagement increases, so do the risks associated with cyber threats. Cybercrimes such as identity theft, online harassment, phishing attacks, and device hacking are becoming more common. These threats can compromise personal data, financial information, and professional work. Protecting digital privacy has therefore become essential for everyone.

Security Issues and Privacy Issues

Cyber hygiene refers to good digital habits that help protect users from cyber threats. Just like personal hygiene protects health, cyber hygiene protects digital identity and data. Key cyber hygiene practices include:1. Using strong and unique passwords,2. Avoiding suspicious links and emails, Regularly updating software and devices,3. Using trusted networks for online transactions, Protecting USB ports and external device access. Women working in offices, remote environments, educational institutions, or public workplaces often use shared computers or systems. In such situations, physical port security becomes extremely important. Physical data security tools help by:1. Preventing unauthorized data copying2. Blocking malware from infected USB drives3. Protecting confidential work files4. Securing shared office computers5. Ensuring safe device usage in public environments.

Promoting Cyber Awareness for Women is essential. Awareness is one of the most powerful tools in cyber security. Educating women about cyber risks and protective measures can significantly reduce vulnerability to cybercrime. Organizations, educational institutions, and technology companies can help by:1Conducting cyber awareness workshops 2. Promoting safe internet practices 3. Encouraging the use of secure devices 4. Providing access to reliable security tools. When women are equipped with knowledge and protective technology, they are better prepared to navigate the digital world safely. Building a Safer Digital Environment is the need of the hour. Cyber security is not just the responsibility of IT professionals—it is a shared responsibility for individuals, organizations, and society. As more women become leaders, entrepreneurs, professionals, and digital creators. Technology companies are contributing to this mission by developing innovative solutions that focus on protecting devices and preventing data breaches. By combining cyber awareness, safe digital habits, and physical data security tools, women can confidently participate in the digital economy without fear of cyber threats.

References

1. Alexandra Michota, Digital security concerns and threats facing women entrepreneurs, Journal of Innovation and Entrepreneurship 2(1),May 2014; DOI:10. 1186/2192-5372-2-7.
2. Acquisti, A, Gritzalis, S, Lambrinoudakis, C, & de Capitani Di Vimercati, S . Digital Privacy. NY: AUERBACHPublications, Taylor and Francis Group, Year-2007.
3. Bonneau, J, Anderson, J, &Danezis, G. Prying data out of a social network. In the first international conference onadvances in social networks analysis and mining (pp. 249–254). Piscataway: IEEE Xplore, Year-2009.
4. Dutta, S, & Bilbao-Osorio, B (Eds.). Global information technology report 2012: living in a hyperconnected world. Geneva: World Economic Forum and INSEAD. Year-2012.
5. Eidlin, F, & Appelbaum, R. Social Science, Social Engineering, and Public Policy. Chicago: American Political ScienceAssociation Proceedings. Year-1983.
6. Gillwald, A. Telecommunication Policy and Regulation for Women and Development. The Southern AfricanJournal of Information and Communication, 1(1),2001.
7. Gross, R, &Acquisti, A. Information revelation and privacy in online social networks (The Facebook case), Pre-proceedings version. Alexandria: ACM Workshop on Privacy in the Electronic Society (WPES). Year-2005.
8. Jones, H, & Soltren, JH (2005). Facebook: threats to privacy. Cambridge, MA: Massachusetts Institute of Technologyhttp://www. swiss. ai. mit. edu/6095/student-papers/fall05-papers/ facebook. pdf. Accessed 10 Sept 2012.
9. Raykova, M, Cui, A, Vo, B, Liu, B, Malkin, T, Bellovin, S, & Stolfo, SJ . Usable, secure, private search. Piscataway:IEEE Security & Privacy, 10(5), 53–60, Year-2012
10. Yang, L, & Yang, SH . A framework of security and safety checking for internet-based control systems. International Journal of Information and Computer Security, 1(1/2), 185–200. Year-2007.

❑❑❑