APAC Cybersecurity Fund

The Asia Foundation

DIGITAL GROWTH, UNEQUAL RISKS

Strengthening Cyber Resilience for Women-Led MSMEs

in partnership with CyberPeace Institute GLOBAL CYBER ALLIANCE

with support from Google.org

Acknowledgments

This report was authored by the CyberPeace Institute, in collaboration with The Asia Foundation and supported by Google.org.

Research

CyberPeace Institute team: Adrien Ogee, Jim Boevink

Project Management

APAC Cybersecurity Fund policy team: Anthea Mulakala, Rukshanie Vidyaratne, Diya Nag, Sandy Walsh, Sharifah Shahirah Idid, Syasya Roslan

Design

Syasya Roslan

Cover photo: Image altered using Canva AI tool.

DIGITAL GROWTH, UNEQUAL RISKS
Strengthening Cyber Resilience for Women-Led MSMEs

KUALA LUMPUR, MALAYSIA, March 2026.

© The Asia Foundation 2026.

All rights reserved. No part of this report may be reproduced without written permission from The Asia Foundation.

Executive Summary

Cybercrime is a systemic risk to the Asia-Pacific region's digital economy, generating billions of dollars in annual losses (UNODC, 2024). Women-led MSMEs, which account for roughly one in three businesses in the region, face distinct exposure to these threats. Yet cybersecurity policy rarely accounts for how gender shapes risk and recovery.

This policy brief examines how cybersecurity threats and scam dynamics specifically affect women-led MSMEs in Asia and the Pacific. It argues that gender is not merely background context, but a critical lens through which cyber risk must be understood. The structural constraints women entrepreneurs face, from reliance on social commerce platforms to limited access to capital for security investments, translate directly into cyber vulnerability pathways that make them disproportionately exposed to fraud, impersonation attacks, and technology-facilitated harassment. The brief provides actionable recommendations for reducing scam exposure, strengthening secure participation in e-commerce, and embedding protections within platforms and payment systems in ways accessible to women-led MSMEs.

Industrial-scale scam operations have proliferated across Southeast Asia, with the United Nations Office on Drugs and Crime reporting that cyber fraud centers now generate nearly USD 40 billion in annual illicit profits, with scams affecting people across the globe (UNODC, 2024). These operations target victims globally through investment fraud, romance scams, and increasingly sophisticated impersonation attacks using AI-generated deepfakes. Women-led MSMEs face particular exposure due to their patterns of digital commerce and structural constraints that limit security investments.

Key Statistics

43%

of all cyberattacks globally target small businesses, which typically lack dedicated IT security resources (Accenture, 2023).

46%

of all small businesses have suffered a cyberattack, **1 of 5** of the affected businesses filed for bankruptcy thereafter (Mastercard, 2025).

Women account for more than half of romance fraud victims globally, and when women lose money to scams, their average losses are significantly higher, averaging **£8,900 per claim** compared to lower median losses for men (Action Fraud, 2024, Barclays, 2024).

A **5-year empirical study** of cybercrime victimization in the Philippines (2020–2024) found that **females and employed adults aged 25 to 59 were the most common victims,** reflecting how women's increasing online activity and financial participation expand their exposure to exploitation (Rufino et al., 2025).

Problem Overview

Structural inequalities are increasing cyber risks for women-led MSMEs

Women entrepreneurs do not face a neutral cyber threat landscape. Gender shapes how they participate in digital markets, how they are targeted, and how cyber incidents affect their businesses. Women-led MSMEs often rely more heavily on social commerce, direct customer engagement, and personal account management, increasing exposure to impersonation, account takeovers, cyber-enabled fraud, and digital harassment.

Gendered online abuse, including coordinated harassment, doxxing, and reputational attacks, can spill over into business harm by undermining customer trust and platform credibility. At the same time, many scam tactics rely on relationship-building and trust exploitation, targeting entrepreneurs seeking capital, suppliers, or new customers. These patterns highlight how structural and social realities intersect with cybersecurity risk, creating distinct vulnerability pathways for women-led businesses.

"After seeing my husband fall victim to a malware attack while using AI tools, and watching friends and even law enforcement officers unknowingly transfer money to the attacker, I realized how vulnerable we all are in the digital space. As vice president in charge of finance, I felt a responsibility to warn our members and ensure they never face the same risks. That is why I immediately alerted everyone through our association's Zalo group and worked with VWEC to organize cybersecurity training. We must stay informed and prepared—because a single incident can affect an entire community."

Ms. Huỳnh Thị Cúc – Vice President of the Da Nang Women Entrepreneurs Association & Director of Thien Minh Digital Photo Enterprise

From Gender Constraints to Cyber Vulnerabilities

The structural barriers facing women entrepreneurs translate directly into specific cyber vulnerability pathways.

Social Commerce Reliance → Platform-Based Threats

Women entrepreneurs in APAC disproportionately operate through social media platforms rather than standalone e-commerce, reflecting both opportunity (lower entry barriers, built-in networks) and constraint (limited capital, time poverty). This reliance increases exposure to account takeover, impersonation, and business page hijacking–where a compromised page means losing an entire storefront, customer base, and reputation.

Limited Capital → Underinvestment in Security

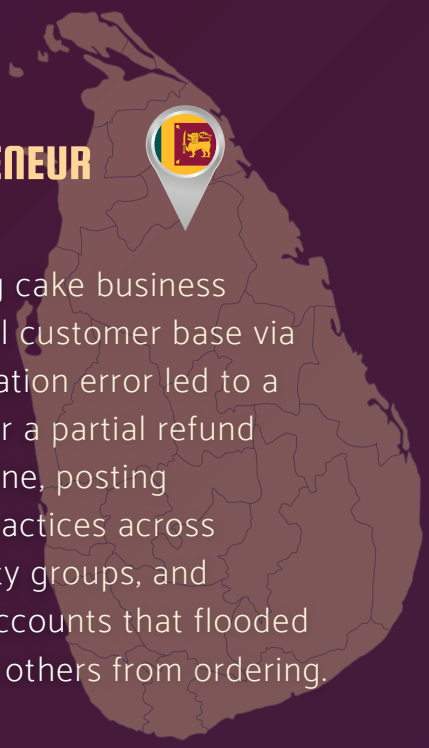
Women-owned MSMEs face significant financing constraints, including an estimated USD 104 billion credit gap in Southeast Asia. Limited formal finance pushes entrepreneurs into informal markets, reducing access to secure payment systems, fraud recovery, and support programs. Constrained capital means women-led MSMEs are more likely to rely on unlicensed software, free-tier platforms with limited security, and unprotected personal devices.

Digital Skills Gap → Reduced Threat Recognition

Women in low and middle income countries are 15% less likely than men to use mobile internet, with 45% of women entrepreneurs lacking regular access due to cost and connectivity barriers (Cherie Blair Foundation, 2025). Lower digital engagement reduces exposure to evolving threat awareness. Where training exists, time constraints, caregiving responsibilities, cultural norms, and curricula that overlook women's broader digital ecosystems limit its effectiveness.

Online Harassment → Business Harm and Withdrawal

Technology-facilitated gender-based violence creates business risks beyond personal harm, with attacks often using misogynistic and sexualized harassment (UN Women & UNU Macau, 2024). Doxxing, coordinated review bombing, and impersonation accounts can force withdrawal from online marketplaces and translate directly into economic harm.



ECONOMIC HARM TO A HOME-BASED CAKE ENTREPRENEUR IN SRI LANKA

A Sri Lankan home-based female entrepreneur ran a growing cake business through Facebook, Instagram, and WhatsApp, building a loyal customer base via photos, testimonials, and word-of-mouth. When a communication error led to a mismatched cake delivery, her attempt to apologize and offer a partial refund failed to satisfy the customer, who escalated the dispute online, posting defamatory accusations of dishonesty and unsafe hygiene practices across multiple platforms, circulating screenshots in local community groups, and ultimately coordinating a harassment campaign using fake accounts that flooded the business page with negative comments and discouraged others from ordering.

Common Cyber Threats Affecting Women-Led Businesses

Cyber threat actors increasingly exploit patterns in women's digital participation, particularly in online commerce environments.

Business Email Compromise and Supplier Impersonation

Scammers monitor business communications and impersonate suppliers or buyers to redirect payments. Women entrepreneurs who manage communications personally may face concentrated verification risk. AI-generated voice and video tools are lowering the barrier to convincing impersonation.

E-commerce Platform Fraud

Fraudulent buyer schemes increasingly target sellers on major regional platforms such as Shopee, Lazada, and Facebook Marketplace. Common tactics include fake payment confirmations, chargeback fraud after goods are shipped, and "task scam" recruitment into fraudulent commission schemes (Singapore Police Force, 2024; FTC, 2025). In Singapore alone, e-commerce scams resulted in SGD 8.6 million in reported losses in the first half of 2024 (Singapore Police Force, 2024).

Investment and Loan Scams

Investment and loan scams increasingly target entrepreneurs seeking business capital. In so-called "pig-butchering" schemes, scammers groom victims through fabricated relationships before directing them to fraudulent investment platforms. Posing as investors or grant administrators, they exploit financing gaps facing women entrepreneurs. In one Hong Kong case (2025), a woman lost nearly HKD2 million after being persuaded via WhatsApp to invest in a fraudulent gold scheme (SCMP, 2025).

Account Takeover and Identity Theft

Phishing attacks targeting social commerce accounts are increasingly sophisticated. According to the Verizon Data Breach Investigations Report (2024), 86% of web application attacks involve stolen credentials. Account takeover can halt sales, erode customer trust, and disrupt business continuity. Recovery processes are often slow, compounding financial loss.

Regional Policy Landscape and Gaps

Regional frameworks increasingly acknowledge links between gender equality, digital economy development, and cybersecurity. However, implementation remains uneven, particularly in protecting women-led MSMEs in digital marketplaces.

Existing Frameworks

Several regional initiatives, including the APEC La Serena Roadmap (2019) and the ASEAN Gender Mainstreaming Strategic Framework (2021-2025), recognize the importance of women's participation in the digital economy. However, cybersecurity and online marketplace risks are not yet systematically integrated into these agendas, and implementation remains limited.

Current Gaps

Despite growing regional recognition, significant implementation gaps remain. Legal pathways for reporting digital fraud and recovering losses are uneven across APAC, and dispute resolution mechanisms are often slow or unclear for small business users. Data systems rarely capture gender-disaggregated cybercrime information, limiting the ability to assess how cyber incidents affect women-led MSMEs specifically. Cross-border enforcement coordination continues to lag behind scam networks that operate across multiple jurisdictions. At the platform level, standards for seller protection, account recovery, and fraud detection vary considerably, leaving small online sellers exposed to prolonged disruption after account compromise or impersonation.

Recommendations

For Governments and Policymakers

- **Strengthen legal and enforcement pathways for MSME** cyber risks, including clearer reporting channels, rapid transaction freezing, and accessible civil redress. Ensure reporting mechanisms account for barriers women disproportionately face, such as time constraints, language, and cultural norms.

- **Require platforms to provide timely account recovery** and local-language support for business users, with processes accessible to informal business operators.

- **Expand digital voucher schemes or subsidies** for secure tools and fraud prevention, with eligibility criteria designed to reach informal and home-based businesses, which are disproportionately women-led.

- **Integrate scam awareness and digital safety into MSME support programs** and channels women already access, such as microfinance onboarding, cooperatives, and women's business associations.

- **Enhance cross-border coordination to disrupt scam networks**, with attention to social commerce platforms where women entrepreneurs are concentrated.

- **Encourage peer-led cybersecurity ambassador models** through women's business associations to share practical scam prevention and recovery knowledge.

For E-commerce and Social Media Platforms

- **Strengthen account verification and provide expedited recovery** for compromised business accounts, accessible in local languages and without documentation requirements that exclude informal operators.
- **Enable secure defaults for business users**, including multi-factor authentication and suspicious activity alerts.
- **Introduce safeguards for high-risk transactions**, including payment verification friction and buyer validation.
- **Improve detection of impersonation, review manipulation, and account takeover,** including gendered attacks such as sexualized impersonation targeting women sellers.
- **Deliver timely in-app scam alerts** at moments of elevated risk, designed for mobile-first and low-bandwidth environments.

For Financial Institutions and Payment Providers

- **Embed scam awareness and fraud prevention guidance** into MSME account onboarding, accessible for mobile-first and low-bandwidth users.
- **Enhance real-time transaction monitoring** and pre-transfer warnings for suspicious payments.
- **Develop affordable risk-sharing mechanisms**, such as bundled micro-cyber insurance, available to businesses outside formal registration systems where women entrepreneurs are overrepresented.

Call to Action

Cyber threats to women-led MSMEs are not an inevitable cost of digital participation. They reflect identifiable gaps in enforcement, platform design, and access to recovery mechanisms that can be addressed through coordinated action.

Women-led MSMEs account for roughly one in three businesses across Asia-Pacific. Their exposure to account compromise, cyber-enabled fraud, digital harassment, and other security risks is shaped by structural realities, including reliance on digital platforms, constrained capital, and time limitations. Securing these businesses is therefore not a niche gender issue, but a matter of business continuity and regional economic resilience.

Strengthening cybersecurity for women-led MSMEs requires embedding gender-aware safeguards into digital ecosystems. Governments, platforms, financial institutions, and development partners each have a role in designing protections that reflect how risk is distributed across the MSME landscape. Integrating gender into cybersecurity design is not an add-on to digital growth. It is foundational to sustaining trust in the region's digital economy.

References

Accenture (2023). State of Cybersecurity Report.

APEC (2019). La Serena Roadmap for Women and Inclusive Growth.

ASEAN (2021). ASEAN Gender Mainstreaming Strategic Framework 2021-2025.

Cherie Blair Foundation for Women (2025). Empowered or Undermined? Women Entrepreneurs and the Digital Economy.

Singapore Police Force (2024). Mid-Year Scams and Cybercrime Brief 2024.

UN Women & UNU Macau (2024). Cybersecurity Threats, Vulnerabilities and Resilience Among Women Human Rights Defenders and Civil Society in South-East Asia.

UNODC (2024). Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking, and Technological Innovation: A Shifting Threat Landscape.

Action Fraud (2024). Romance fraud statistics by gender. UK National Fraud & Cyber Crime Reporting Centre.

Barclays (2024). Scams Bulletin: Men more likely to fall victim to romance scams, while women lose more money.

FTC (2025). Consumer Sentinel Network Data Book 2024.

Rufino, R. and Moyao, M. (2025). Five-Year Empirical Analysis of Cybercrime Victimization Trends in Pangasinan, Philippines. International Journal of Research and Innovation in Social Science.

SCMP (2025). Hong Kong woman loses nearly HK$2 million in 'pig butchering' romance scam.

Mastercard (2025). Too small to be ignored? Not anymore. Why shoring up cyber defenses for small businesses is crucial.

Verizon (2024). Data Breach Investigations Report.

The APAC Cybersecurity Fund

The APAC Cybersecurity Fund is an initiative by The Asia Foundation, supported by Google.org, Google's philanthropic arm, designed to build inclusive and sustainable cybersecurity ecosystems across the Asia-Pacific region. Through cyber hygiene training, policy research, and stakeholder engagement, the program helps micro and small businesses, nonprofits, and social enterprises strengthen their cyber resilience. It also invests in long-term capacity by establishing more than 20 university-based cyber clinics to expand outreach and develop the region's cybersecurity workforce. The initiative spans 13 countries including Australia, Bangladesh, India, Indonesia, Japan, Korea, Malaysia, Pakistan, Philippines, Singapore, Sri Lanka, Thailand, and Vietnam.

CyberPeace Institute

The CyberPeace Institute protects the most vulnerable in cyberspace. We deliver cybersecurity assistance and hold all actors accountable for ensuring peace in cyberspace by exposing the human harm caused by cyberattacks and disinformation. We advocate against the unacceptable use of artificial intelligence to threaten international peace and security, while promoting the responsible development and use of AI.

The Asia Foundation

The Asia Foundation is an international nonprofit organization working to solve the toughest social and economic challenges in Asia and the Pacific. Informed by more than 70 years of experience and deep local knowledge, we work with partners across more than 20 countries to improve lives and expand opportunities.

Google.org

Google.org, Google's philanthropy, brings the best of Google to help solve some of humanity's biggest challenges combining funding, product donations, and technical expertise to support underserved communities, and provide opportunity for everyone. We engage nonprofits, social enterprises and civic entities who make a significant impact on the communities they serve, and whose work has the potential to produce scalable, meaningful change.

with support from

Google.org

in partnership with

CyberPeace Institute

GLOBAL CYBER ALLIANCE

The Asia Foundation

The Asia Foundation
www.asiafoundation.org

© The Asia Foundation 2026