



INVISIBLE THREATS, VISIBLE IMPACT

Securing MSMEs in the Scam Economy

Overview:

Across Asia-Pacific, MSMEs are rapidly adopting e-commerce and digital platforms to expand market access, reach customers, and drive growth. This transition enables economic opportunity but also exposes businesses to rising cyber risks, including scams, fraud, impersonation, and account compromise. Limited cybersecurity capacity, reliance on informal selling channels, and weak digital safeguards increase vulnerability across the MSME sector.

The result is a dual dynamic:

E-commerce enables MSME growth by:

- Expanding access to domestic and global markets
- Lowering entry barriers through digital platforms
- Enabling mobile-first and social commerce models
- Driving post-pandemic economic recovery

But it also increases exposure to:

- Fraudulent transactions and scams
- Identity theft and impersonation
- Platform and payment vulnerabilities
- Systemic risks across digital supply chains

Key message:

Digital growth without security creates structural risk. MSMEs are the most exposed actors in the digital economy.



Cyber Threat Landscape

- **Fraudulent transactions & fake buyers:** Scammers exploit e-commerce platforms through fake orders, payment scams, and non-delivery schemes that result in direct financial losses.
- **Account takeover & phishing:** Weak passwords, phishing attacks, and poor authentication practices enable attackers to gain access to business accounts and customer data.
- **Brand impersonation & counterfeit listings:** Fake storefronts, copied branding, and impersonation accounts undermine customer trust and damage MSME reputations.
- **Ransomware & operational disruption:** Cybercriminals lock businesses out of systems and data, disrupting operations and demanding financial extortion payments.

Structural Vulnerabilities

- **Platform dependence:** Many MSMEs rely heavily on a single e-commerce or social commerce account to manage sales, payments, and customer engagement.
- **Limited cybersecurity capacity:** Small businesses often lack the financial resources, technical expertise, and dedicated staff needed to implement strong cyber protections.
- **Low cyber awareness:** Limited exposure to cybersecurity training reduces the ability of MSMEs to identify scams, phishing attempts, and suspicious online activity.
- **Cross-border enforcement gaps:** Scams frequently operate across jurisdictions, while fragmented reporting and enforcement mechanisms delay response and accountability.

Recommendations



FOR MEDIUM, SMALL AND MICRO ENTERPRISES (MSME)

- Enable multi-factor authentication (MFA)
- Use trusted, platform-based payment systems
- Train staff to recognise scams and phishing
- Back up critical data and update systems regularly
- Monitor online presence and respond to threats



FOR REGIONAL COLLABORATION

- Establish shared scam intelligence and reporting platforms
- Develop minimum regional standards for scam response
- Support cybersecurity capacity building in emerging markets
- Strengthen coordination between governments, platforms, and financial institutions



FOR E-COMMERCE AND DIGITAL PLATFORMS

- Deploy AI-enabled fraud detection systems
- Strengthen seller verification and account protection
- Remove fake listings, impersonation, and counterfeit sellers
- Provide real-time alerts and seller training modules
- Enable safer payments and dispute resolution systems



FOR GOVERNMENTS & POLICYMAKERS

- Launch MSME-focused cybersecurity awareness campaigns
- Provide subsidies/incentives for secure tools
- Strengthen laws addressing e-commerce fraud and scams
- Support cross-border data sharing and enforcement
- Develop digital trustmark systems for small sellers

Call to Action

E-commerce is a major driver of inclusive growth, but digital expansion without security is creating structural risk for MSMEs. Protecting small businesses requires coordinated action across governments, platforms, and regional ecosystems. Embedding cybersecurity into digital commerce will help strengthen trust, reduce fraud, and ensure that MSMEs can participate safely and sustainably in the digital economy.



APAC Cybersecurity Fund



The Asia Foundation



Learn more about how rapid e-commerce adoption is transforming MSMEs across Asia and the Pacific, creating new opportunities for growth and market access while exposing businesses to rising scams, fraud, and cybersecurity risks.

DOWNLOAD NOW

www.apaccyberfund.com

in partnership with



Protect.ngo



**GLOBAL
CYBER
ALLIANCE.**

with support from

Google.org