Capacity Building Workshop Report

Cyber Security Capacity Building Workshop for MSMEs in India
June 19, 2025, Kokrajhar, Assam

CUTS International, in collaboration with the Department of Industries and Commerce, Government of Assam, organised a cybersecurity workshop for Micro, Small, and Medium Enterprises (MSMEs) in Kokrajhar on 19 June 2025. Supported by The Asia Foundation and Google.org under the APAC Cybersecurity Fund initiative, the workshop aimed to enhance MSMES' digital resilience by building their capacity to identify, prevent, and respond to cybersecurity threats.

The workshop drew the participation of 148 individuals, including entrepreneurs and workers from various parts of the Kokrajhar district. Attendees represented a diverse range of sectors, including garments, food processing, dairy, and stationery, reflecting the region's diverse economic landscape.

Shri Subham Ghosh, Programme Associate, CUTS International, began the session by welcoming the distinguished guest and participants. This was followed by brief remarks by Sri Rohiteshwar Narzary, GM, DICC, Kokrajhar.

Sri Rohiteshwar Narzary highlighted the growing vulnerability of MSMEs, particularly in districts like Kokrajhar, to cyber threats such as phishing, ransomware, and data breaches. He attributed this rising risk to limited technical capabilities and low cybersecurity awareness among small business owners. Emphasizing the urgent need for targeted interventions, he stressed that as MSMEs increasingly adopt digital platforms, strengthening their cyber resilience has become critical.

The workshop was designed to address these challenges by equipping participants with essential knowledge, practical tools, and preventive strategies. By fostering cybersecurity awareness and promoting safe digital practices, the initiative aims to enhance the preparedness of MSMEs in Kokrajhar, enabling them to counter emerging cyber risks effectively.

The cybersecurity workshop attracted 148 participants, with a significant majority (80 attendees) representing MSMEs and the remaining comprising representatives from NGOs, business associations, and related organisations. The participants were predominantly between the ages of 35 and 42, with most having completed at least secondary education. A significant lack of awareness regarding cybersecurity threats emerged during the sessions, although three participants shared that they had previously encountered cyberattacks.

The workshop focused on building cybersecurity awareness among MSME owners, staff, and business partners by covering a broad spectrum of digital threats, from obvious dangers to often-ignored weak points. Through engaging and interactive sessions, participants were introduced to core cybersecurity practices such as using strong passwords, backing up data regularly, updating software on time, and managing digital assets effectively. To keep the sessions lively and reinforce key takeaways, quizzes were held at the end of each segment, with participants actively responding and receiving prizes for correct answers. This format not only deepened understanding but also created an energetic, hands-on atmosphere that promoted real-world application of cybersecurity practices.

Analysis of participants' feedback after the workshop illustrated that 80 of them rated the workshop as highly relevant and expressed strong appreciation for the quality of the content and the practical value of the case studies presented. 76 participants termed their experience as positive and indicated interest in attending future cybersecurity workshops.

One participant recounted receiving an SMS posing as a government agency, claiming their Aadhaar card (or similar ID) was "suspended due to irregularities." The message included a fraudulent link to "verify details immediately" to avoid penalties. Recognising the urgent tone and grammatical errors in the message, the participant became suspicious. Instead of clicking the link, they cross-checked the official government website and discovered it was a phishing scam designed to steal sensitive data. They promptly reported the incident to the National Cyber Crime Portal and alerted their peers. This case highlights how cybercriminals exploit trust in official institutions, leveraging urgency and fear to manipulate victims. It also underscores the importance of verifying information through official channels before taking action.

Workshop Glimpses of the training sessions and Group Photo

Cybersecurity Capacity Building
Workshop for MSMEs in India
As part the APAC Cybersecurity Fund Project
ASSAM

Cybersecurity Capacity Building
Workshop for MSMEs in India
As part the APAC Cybersecurity Fund Pr