

Capacity Building Workshop Report

Cyber Security Capacity Building Workshop for MSMEs in India **June 11, 2025 | Chirang, Assam**

In collaboration with the Department of Industries and Commerce, Assam, CUTS International conducted a cybersecurity workshop for MSMEs on June 11, 2025, in Chirang. The event, supported by The Asia Foundation and Google.org, was organised under the APAC Cybersecurity Fund initiative, which aims to enhance digital resilience among small businesses.

The workshop brought together entrepreneurs and workers from different places of the Chirang district, representing diverse industries such as garments, food processing, artisans, dairy, stationery, poultry and others. The workshop attracted 125 participants.



Shri Subham Ghosh, Programme Associate, CUTS International, began the session by welcoming the distinguished guest and participants. This was followed by brief remarks by Shri Bikram Kalita, General Manager, DICC, Chirang

Shri Bikram Kalita, General Manager of DICC Chirang, highlighted the growing vulnerability of MSMEs in Assam, particularly in districts like Chirang, to cyber threats such as phishing, ransomware, and data breaches, primarily due to

limited technical resources and awareness. He emphasised the critical need for targeted cybersecurity interventions to protect these enterprises as they increasingly adopt digital platforms. The workshop aims to address this gap by equipping MSME participants with essential knowledge, practical tools, and preventive strategies to strengthen their cyber resilience. By fostering awareness and promoting safe digital practices, the programme is expected to enhance the overall preparedness of Chirang's MSMEs against evolving cyber risks.

The cybersecurity workshop attracted 125 participants, with a significant majority (77 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. Despite this knowledge gap, the workshop sparked notable enthusiasm, with the majority of attendees expressing a strong willingness to implement cybersecurity practices within their organisations. This reflects a positive and encouraging shift towards understanding the vital role of digital protection in ensuring business continuity and resilience..

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 87 of them (70 per cent) 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. 70 participants (56 per cent) termed their experience as positive and indicated interest in attending future cybersecurity workshops.

During the cybersecurity workshop held in Chirang, a compelling case emerged involving Mamoni Basumatary, a female entrepreneur from the district, who had recently fallen victim to a phone-based cyber fraud. She received a call from someone posing as a bank official, warning her of immediate account suspension unless she verified her banking credentials. Trusting the caller, Mamoni unknowingly shared her OTP, which led to unauthorised access and withdrawal of funds from her account. Her story, shared during the workshop, served as a powerful real-world example of how easily individuals can be misled in the absence of cybersecurity awareness. Her experience not only highlighted the growing threat of social engineering scams but also reinforced the importance of such workshops in equipping MSME stakeholders with the knowledge to identify and avoid similar attacks.

Workshop Glimpses of the training sessions and Group Photo



with support from **Google.org**