Capacity Building Workshop Report

Cyber Security Capacity Building Workshop for MSMEs in India
May 22, 2025 | Barasat, North 24 Parganas, West Bengal

CUTS International organised a cybersecurity workshop for MSMEs in Barasat, North 24 Parganas, West Bengal, in collaboration District Industries Centre, North 24 Parganas with on May 22, 2025. Supported by The Asia Foundation and Google.org, the event was part of the APAC Cybersecurity Fund initiative to strengthen digital security among small businesses.

The workshop brought together entrepreneurs and workers from different places of the North 24 Parganas district, representing diverse industries such as garments, food processing, artisans, tailoring, jewellery, exporters, importers and others. The workshop attracted over 140 participants.

Shri Pratyush Banerjee, Programme Associate, CUTS International, began the session by welcoming the distinguished guests and participants. This was followed by brief remarks by Shri Sumit Chatterjee, General Manager, DIC, North 24 Parganas, Shri Sharad Kumar Dwivedi, IAS, District Magistrate & Collector, North 24 Parganas, Shri Manish Mishra, IAS, Addl. District Magistrate (General) & ADM (Industry`), North 24 Parganas, Shri Vidyagar Ajinkya Anant, IPS, SDPO, Barasat, North 24 Parganas, Shri Chiranjeeb Ghosh, President, District Chamber of Commerce and Industry, Shri Manoj Pandey, Secretary, District Chamber of Commerce and Industry.

Shri Sumit Chatterjee, General Manager of the District Industries Centre (DIC), highlighted the increasing relevance of cybersecurity for MSMEs, noting that digital threats are no longer confined to large enterprises. He emphasised that smaller businesses, often lacking robust cybersecurity infrastructure, are becoming frequent targets of cyberattacks. Drawing on practical examples, he urged stakeholders to adopt preventive measures, strengthen cyber hygiene practices, and remain vigilant. His remarks underscored the need for enhanced awareness and capacity-building at the grassroots industrial level

The workshop had 142 participants, out of which 110 were MSMEs, and the rest were from non-

government organisations, business associations, and similar entities. Most participants belonged to the age group of 35-42 years and had completed secondary or high school education. Many of them expressed a lack of adequate knowledge of cybersecurity issues. 49 individuals indicated they have previously experienced cyberattacks. Most of the participants expressed a strong willingness to adopt and implement cybersecurity practices in their respective businesses.

The workshop aimed to sensitise MSME owners, employees, and business associates to various cyber security threats, ranging from the easily identifiable to the more subtle and often ignored. Sessions covered essential topics such as the basics of cyber security, the role of strong and unique passwords, and the need for regular data backups, timely software updates, and efficient inventory tracking. To reinforce learning and encourage engagement, each session concluded with a quiz. Participants actively took part, showcasing their understanding and winning prizes for correct responses.

Analysis of participants' feedback after the workshop illustrated that 130 of them (92 percent) 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. 125 participants (88 percent) termed their experience as positive and indicated interest in attending future cybersecurity workshops.

One of the workshop participants shared a recent personal experience in which his WhatsApp account was compromised by a cyber attacker, who gained unauthorised access and began impersonating him to communicate with his contacts. The attacker attempted to manipulate recipients, including clients and business associates, putting both personal and professional relationships at risk. The participant had to act quickly to report the incident, recover his account, and notify his network about the breach. This incident highlighted the vulnerability of widely used digital platforms and the urgent need for preventive measures such as two-factor authentication, awareness of phishing tactics, and regular monitoring of digital accounts. His experience was a powerful reminder for fellow MSME stakeholders of the real and growing threat of cyberattacks, even through everyday communication tools.

One of the participants shared a troubling cybercrime experience in which he attempted to place a bulk order for TMT steel bars through what appeared to be a reputed supplier's website. The site looked professional and trustworthy, prompting him to make a substantial payment. However, after the transaction, he received no confirmation or delivery, and his attempts to contact customer support were unsuccessful. Upon filing a complaint with the regional cybercrime department, he discovered that the website was fake, designed to mimic a legitimate business using subtle domain name changes and fraudulent payment gateways. This incident underscores the importance of verifying website authenticity, using secure payment methods, and promptly reporting suspicious activity to avoid falling victim to such scams.

Workshop Glimpses of the training sessions and Group Photo

with support from Google.org