Council for Social & Digital Development

Cyber Shakti

Cyber Safe Business for Women Entrepreneurs

Background & Rationale

With the rise of digital transactions and online businesses, cybercrime has surged, particularly affecting women entrepreneurs who lack cybersecurity awareness. The National Crime Records Bureau (NCRB) 2022 report highlights a 24.4% increase in cybercrimes, with financial fraud, phishing, and social media scams being the most prevalent.

States like Assam and other Northeastern regions have witnessed a concerning rise in cybercrimes, with women entrepreneurs being disproportionately affected due to limited awareness and cybersecurity measures.

In Northeast India, cases such as:

- A woman entrepreneur in Assam lost ₹1.5 lakh to a phishing scam.
- A Manipur-based handicraft seller fell victim to a fake buyer scam, leading to malware infection and data theft.

The above incidents demonstrate the urgent and continuous need for cyber safety training for women entrepreneurs, in urban and rural areas, especially in Assam and the North East Region, where women entrepreneurs attempt to rise and grow in their businesses and become part of the digital economy.

Cyber Shakti aims to bridge this gap by providing **practical, hands-on cybersecurity training tailored** for women entrepreneurs in Assam and North East India.

'Cyber Shakti'

'Cyber Shakti' is an initiative designed to equip rural and urban women entrepreneurs with the knowledge and skills to safely navigate the digital business landscape. The program focuses on preventive and curative cybersecurity measures, ensuring that women-led businesses can operate online without falling victim to scams, financial fraud, or data breaches.

Project Objectives

- Educate women entrepreneurs on cyber threats in online business.
- Equip them with preventive and curative measures against fraud.
- Build confidence in digital transactions and e-commerce.
- Reduce financial losses due to cybercrime.

Target Beneficiaries

- Women entrepreneurs (small business owners, SHG enterprises, Nano and micro women entrepreneurs and enterprises).
- Women engaged in digital payments, e-commerce, or social media marketing.
- Aspiring entrepreneurs transitioning to an online business.

Expected Outcomes

- Increased awareness of cyber threats among rural women entrepreneurs.
- Adoption of secure digital business practices.
- Reduction in financial losses due to cyber fraud.
- Stronger trust in online business operations.
- Empowerment of women to confidently operate cyber-safe businesses.

Cyber Shakti

Monitoring & Evaluation

Pre - workshop assessments

Workshop wih Modules

Post-workshop assessments

Follow-up surveys

Case studies

Case studies of participants who prevented fraud post-training.

Sustainability & Scalability

- Local partnerships with women's SHGs, banks, and cyber police.
- Digital resource hub for ongoing learning.
- Potential expansion to other states with high cybercrime rates.

Cyber Shakti Reach

- Cyber Shakti has conducted multiple training sessions with women entrepreneurs.
- The initiative has reached out to **1,800 women entrepreneurs across 12 districts** in Assam.
- These sessions aim to **build capacities in women entrepreneurs and enterprises** to conduct business safely in the digital economy.
- The trainings focus on a **combination of awareness, prevention, and practical skills.**
- They are helping to ensure **long-term resilience against cyber threats for women-led businesses.**

‘Cyber Shakti’ Activities

Phase 1: Workshop Modules

Module 1: Introduction to Cyber Safe Business

- What is a Cyber Safe Business?
- Examples of online business risks (e-commerce fraud, payment scams).
- Why cybersecurity is critical for rural entrepreneurs.

Module 2: Common Cyber Threats (With Case Studies)

- Phishing (Fake UPI links, impersonation scams).
- Hacking (Social media account takeovers).
- Financial Fraud (Fake loan apps, QR code scams).
- Ransomware & Malware (Data theft risks).

Module 3: Preventive & Curative Measures

- Secure passwords & Two-Factor Authentication (2FA).
- Safe digital payment practices.
- How to report cybercrime (via Cybercrime Portal).
- Steps to recover hacked accounts.

Phase 2: Interactive Sessions

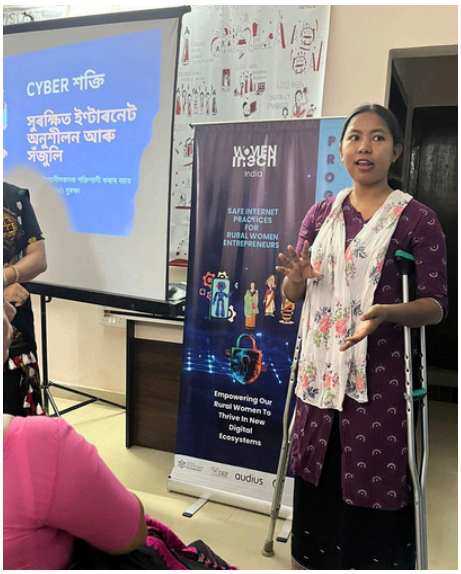
- Live phishing attack demo (How to spot fake messages).
- Hands-on exercises (Securing WhatsApp/Facebook business accounts).
- Simulated cyberattack scenarios (e.g., identifying fake UPI payment requests).
- Group discussions on real-life case studies.

Case study discussions (Real fraud incidents from NE India).

Phase 3: Resource Distribution & Follow-up

- Cyber Safe Toolkit (Checklists, helpline numbers).
- Posters & Flyers (Visual cybersecurity tips).
- Pre & Post-Assessment Surveys (Impact measurement).

Gallery



Cyber Shakti

Council for Social & Digital Development

North East Development Foundation