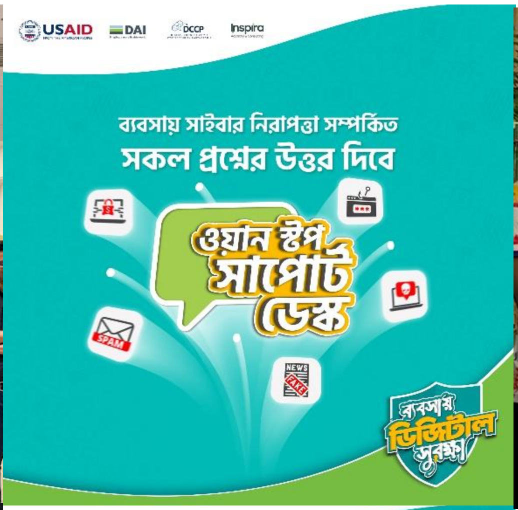
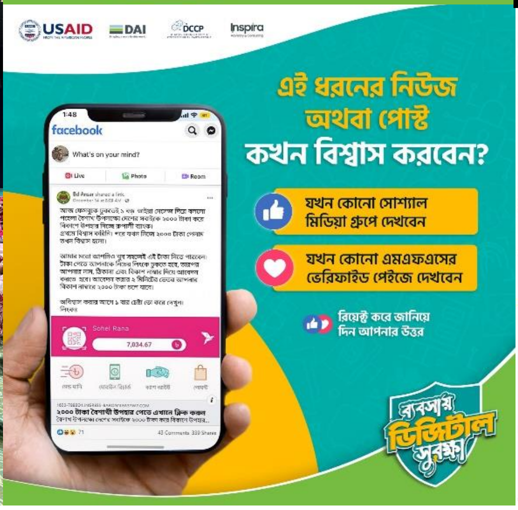




USAID
DAI
DCCP
Inspira
facebook
এই ধরনের নিউজ
অথবা পোস্ট
কখন বিশ্বাস করবেন?
যখন কোনো সোশ্যাল মিডিয়া গ্রুপে দেখবেন
যখন কোনো এমএফএসের ভেরিফাইড পেইজে দেখবেন
রিয়েক্ট করে জানিয়ে দিন আপনার উত্তর
ব্যবসায় ডিজিটাল সুরক্ষা

USAID FROM THE AMERICAN PEOPLE

DCCP DIGITAL CONNECTIVITY & CYBERSECURITY PARTNERSHIP

CAMPAIGN RESULTS & FINAL REPORT

Cybersecurity Awareness for MSMEs in Bangladesh

This report is made possible by the generous support of the American people through the United States Agency for International Development (USAID). The contents are the responsibility of Inspira Advisory & Consulting and do not necessarily reflect the views of USAID or the United States Government.

DAI Shaping a more livable world.

Inspira Advisory & Consulting

Acknowledgment

The Inspira Advisory & Consulting Limited project team would like to thank USAID/Bangladesh and DAI Global, LLC for commissioning this project to us and for the extensive support throughout the design, assessment, and delivery process.

Our sincerest gratitude particularly to Ms. Aklima Haque, Project Management Specialist (Private Sector Development), The Office of Economic Growth, USAID/Bangladesh, Ms. Christin Coster, Senior Program Manager, Digital Frontiers, Benjamin Harguth, Principal Manager - Cybersecurity & Digital Policy Practice and Ms. Komal Bazaz Smith, Digital Connectivity & Cybersecurity Partnership Project Director, Digital Frontiers, for their valuable feedback and support throughout the design and execution of this assessment.

The Inspira team is also grateful to the E-commerce Association of Bangladesh (E-CAB), Women and E-commerce Trust Bangladesh (WE), and Bangladesh Open-Source Network (BDOSN) as long-term partners of the campaign, and to the other collaborating organizations without whom the campaign would not be successful.

We would also like to express our sincerest gratitude to the survey respondents, focus group discussion (FGD) participants, and key informants from the relevant departments of the Government of Bangladesh, implementing partners, ecosystem actors, subject experts, and most importantly the micro, small and medium enterprises (MSMEs) for their valuable insights, which helped us shape the key findings and recommendations of this report.

Acronyms

a2i	Aspire to Innovate
AIDA	Attention, Interest, Desire, Action
B2B	Business-to-Business
CCAF	Cyber Crime Awareness Foundation
COVID-19	Coronavirus disease 2019
DMP	Dhaka Metropolitan Police
e-CAB	E-commerce Association of Bangladesh
ERP	Enterprise Resource Planning
FGD	Focus Group Discussion
FMCG	Fast-Moving Consumer Goods
FnF	Friends and Family
ICT	Information and Communication Technology
KAP	Knowledge, Attitude, Practice
MFA	Multi-Factor Authentication
MFS	Mobile Financial Services
MSME	Micro, Small, and Medium
OS	Operating System
OTP	One Time Password
P2P	Peer-to-Peer
RMG	Ready Made Garments
SARDI	South Asia Regional Digital Initiative
SME	Small and Medium Enterprise
TG	Target Group
USAID	United States Agency for International Development
CWCCI	Chittagong Women Chamber of Commerce and Industry
BdOSN	Bangladesh Open Source Network
WE	Women and E-commerce trust

Executive Summary

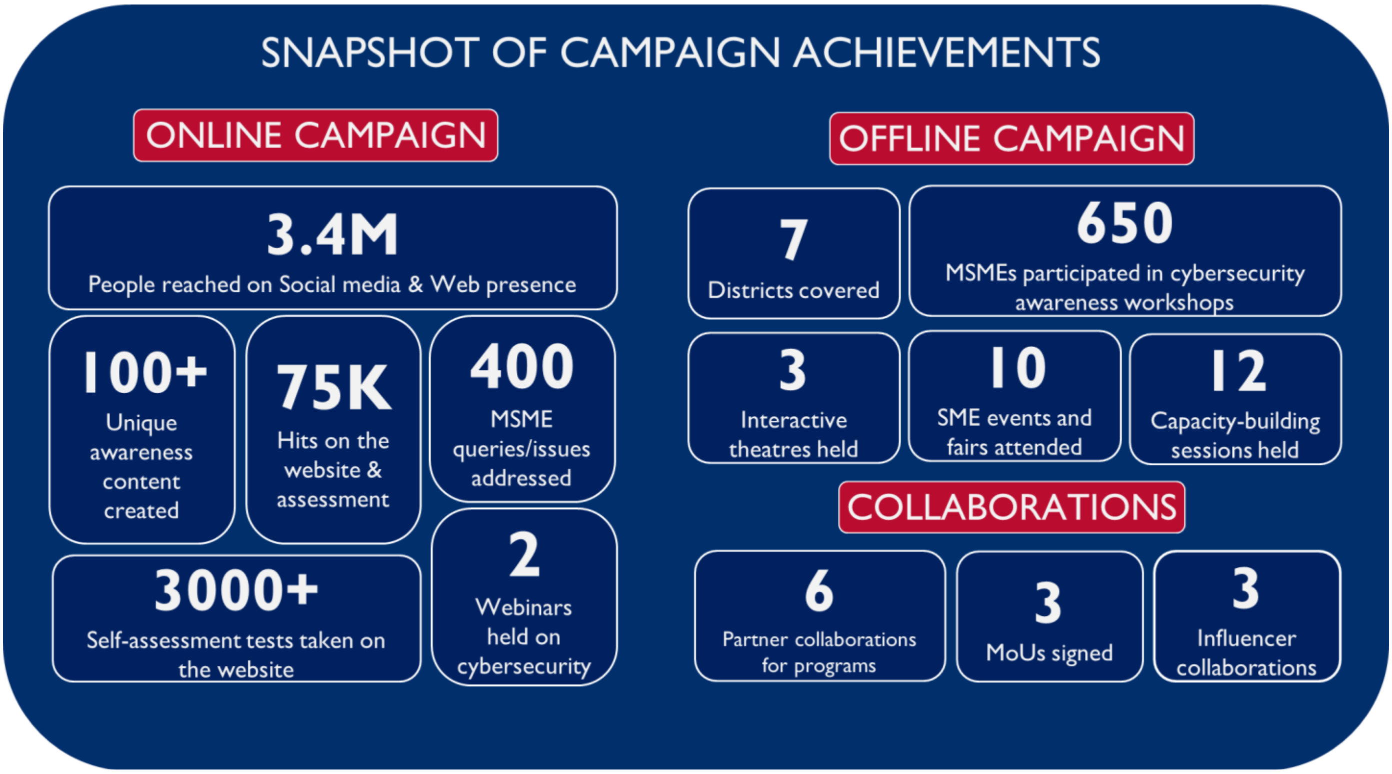
MSMEs in Bangladesh have gradually adopted IT-enabled services and digital tools since the early 2010s. The COVID-19 pandemic further accelerated this digital transformation as traditional MSMEs turned to digital tools and online platforms to sustain their operations. Urban and rural youth also emerge as online entrepreneurs, leveraging social media and e-commerce platforms. However, amidst this rapid shift, MSMEs in Bangladesh have limited knowledge about cybersecurity threats and preventive measures. Many MSME entrepreneurs come from rural communities with little formal education, resulting in a nascent understanding of the cyber world. Consequently, they often fall victim to cyber threats, leading to significant business losses. To address this issue, under USAID's South Asian Regional Digital Initiative (SARDI), the Cybersecurity Awareness Campaign for MSMEs aims to enhance the cybersecurity practices of Bangladeshi MSME owners and improve their personal and business-related digital hygiene.

As part of SARDI, the “Bebshay Digital Shurokkha”[1] campaign was run in Bangladesh from October 2022 to June 2023. Broadly, this campaign aimed to achieve three goals:

I. To raise awareness among business owners regarding cybersecurity concepts and common threats.
II. To improve entrepreneurs’ knowledge regarding cybersecurity best practices to keep their businesses safe.
III. To enhance the capacity of entrepreneurs to respond to cyber threats they face.

Highlights of campaign activities and achievements:

The “Bebshay Digital Shurokkha” Campaign followed a 3-pronged strategy for creating awareness using online mediums to raise mass awareness, conducting offline activations to create a more personal experience for specific sections of the target audience of SME owners, and using partnerships and collaborations to integrate our activities with the broader MSME ecosystem. The notable activities and achievements under each element have been highlighted:



SNAPSHOT OF CAMPAIGN ACHIEVEMENTS

ONLINE CAMPAIGN

3.4M
People reached on Social media & Web presence

100+
Unique awareness content created

75K
Hits on the website & assessment

400
MSME queries/issues addressed

3000+
Self-assessment tests taken on the website

2
Webinars held on cybersecurity

OFFLINE CAMPAIGN

7
Districts covered

650
MSMEs participated in cybersecurity awareness workshops

3
Interactive theatres held

10
SME events and fairs attended

12
Capacity-building sessions held

COLLABORATIONS

6
Partner collaborations for programs

3
MoUs signed

3
Influencer collaborations

Figure 1: Snapshot of Campaign Achievements

[1] “Bebshay Digital Shurokkha” is a Bangla phrase that literally means “Digital safety in business” and was chosen as the name for the campaign to establish immediate relevance to online entrepreneurs.

Online Activities:

1. The online campaign was run on four media platforms: Facebook, YouTube, LinkedIn, and Instagram. Each platform had a different approach, but the core focus was on Facebook since that is where our target audience spends the most time. The **campaign reached 3.4 million people online** through various engagement posts.
2. A dedicated website[2] for the campaign features a large pool of localized cybersecurity awareness content. This resource pool addressed a significant gap in Bangladesh, as most available cybersecurity content did not reflect local problems and context. **Over 100 unique awareness contents have been created under this campaign** through blogs, posters, comic panels, short videos, and more. This content repository will continue to serve people beyond the project timeline.
3. The website also features a self-assessment quiz, which entrepreneurs can take to understand their current cybersecurity knowledge and where their gaps are. The **website itself has had 75,000+ visits** throughout the campaign.
4. **2 webinars and 4 live Q&A sessions were conducted throughout the campaign**, featuring notable cybersecurity experts, important SME community members, and cyber law enforcement officials.
5. The campaign's "One-Stop Support Desk" initiative, created to address any queries or issues SME owners face, was launched in a pilot capacity. **Over the final quarter of the campaign, the OSD, which acts like a cyber helpline, assisted 400 entrepreneurs** by answering their cybersecurity-related queries or resolving cyber threats that had affected them.

Offline Activities:

1. On 26th October 2022, for the inauguration of the "Bebshay Digital Shurokkha" campaign, a launch event was held at the Daily Star Conference Hall. More than 20 key stakeholders, including USAID representatives, government officials, law enforcement, private sector organizations, cybersecurity professionals, legal experts, media, and other notable ecosystem members, joined a round table discussion to share their insights into the cybersecurity needs and gaps of SMEs in Bangladesh, and what can be done to strengthen the security of the online business ecosystem.
2. In collaboration with various ecosystem members, 12 awareness workshops were conducted under the campaign. **650 SME owners participated in the workshops, with around 75% of the entrepreneurs being women. The workshops covered 7 key economic districts:** Dhaka, Narayanganj, Gazipur, Chattogram, Cox's Bazar, Bogura, and Jashore.
3. Notably, a pre-assessment and post-assessment of the cybersecurity knowledge of workshop participants was undertaken. On average, **60% of participants scored below 5 (failing score)** on the test before participating in the workshop. After the workshop, **the fail rate was less than 10%**, indicating that the workshops effectively raised basic cybersecurity awareness.
4. The campaign also undertook a few innovative approaches to awareness raising. The campaign team created a customized "Snakes and Ladders" board game featuring cybersecurity messaging integrated into the gameplay. **Around 800 of these game boards have been distributed among SMEs.**
5. **The campaign team also visited 10 SME fairs and events** and interacted with SME owners to promote the campaign. Alongside attending fairs, the campaign also saw the execution of **3 interactive community theater sessions (Gambhira)**. Over the campaign, the team has interacted directly with over 2000 enterprise owners.

Partnership and Collaborations:

1. The campaign **signed 3 MoUs with important ecosystem actors** to further cybersecurity awareness goals among SMEs. The MoU partners are The E-Commerce Association of Bangladesh (E-CAB)

[2] (Bebshay Digital Shurokkha, n.d.)

CAB), The Women and E-commerce Trust (WE), and the Bangladesh Open-Source Network (BDOSN). Under the partnerships, the campaign conducted joint workshops and awareness sessions for member SMEs and executive committee members of the organizations.

2. Besides the signed partners, the campaign also collaborated with organizations such as the SME Foundation, Chittagong Women Chamber of Commerce and Industries (CWCCI), and Bogura Chamber of Commerce and Industries (BCCI) to arrange awareness programs.
3. **3 influencer collaborations were done under the campaign** to create interesting, dynamic content for greater online audience engagement.

Key Lessons Learned:

- **Partnerships and collaborations are key to amplifying awareness messaging.** Bringing important ecosystem actors into campaign programming ensures two things: establishing relevance and reach. Effective partnerships can assist in ensuring that the messaging is relevant to the target audience, and partner channels and voices can be used to amplify the messages.

- **Having two-way communication with the audience: Constant audience feedback and room for adaptation should be considered** in campaign planning. Awareness is a two-way avenue: the needs and tastes of audiences are always changing.

- **Collaborating with interesting content creators:** Interest creators have existing platforms and large audiences. Using them leads to creating content that the audience is already familiar with and is less time-consuming.

- **Converting beneficiaries into campaign spokespersons:** Businesspeople tend to learn from other businesspeople. Using this insight, the campaign used initial beneficiaries and workshop attendants as promoters and spokespersons. When people realize that any content has helped people with similar needs, they are immediately more likely to explore the topic independently.

Table of Contents

List of Figures

List of Tables

Part 1

CONTEXT

1.0 Context

1.1 Background of the Study

In an age where the global economy is intricately intertwined with the digital realm, the importance of cybersecurity cannot be overstated. The proliferation of the internet and the rapid digitalization of business operations have unlocked unprecedented opportunities for Micro, Small, and Medium-sized Enterprises (MSMEs) in Bangladesh. However, this digital revolution has exposed them to an ever-growing array of cyber threats.

MSMEs, often referred to as the backbone of Bangladesh's economy, contribute significantly to economic growth, job creation, and innovation. Yet, their limited resources, knowledge, and infrastructure make them particularly vulnerable to cyberattacks. With the increasing sophistication of cybercriminals and the dynamic nature of cybersecurity threats, it became imperative to address this vulnerability and empower MSMEs with the necessary knowledge and tools to protect their businesses online.
The "Bebshay Digital Shurokkha" (Digital Business Security) Campaign emerged as a response to this pressing need. This project was conceptualized with the vision of enhancing the digital resilience of MSMEs by equipping them with comprehensive cybersecurity awareness and skills. By doing so, it aimed to foster a secure digital environment where MSMEs could thrive and expand their online presence without fear of cyber threats.

Recognizing the urgent need to address this issue, a campaign has been launched funded by the U.S. Agency for International Development (USAID), and an initiative of the South Asia Regional Development Initiative (SARDI), and being implemented by the Development Alternatives Inc. DAI, aimed at equipping MSME owners and employees with the knowledge and skills to defend against cyber threats.

Recognizing the urgent need to address this issue, a campaign has been launched funded by the U.S. Agency for International Development (USAID), and an initiative of the South Asia Regional Development Initiative (SARDI), and being implemented by the Development Alternatives Inc. DAI, aimed at equipping MSME owners and employees with the knowledge and skills to defend against cyber threats.

1.2 Campaign Objectives against Geographic and Sectoral Scope

The campaign has been undertaken in seven districts of economic significance. The districts were selected based on the following criteria:

- Have a high concentration of targeted MSMEs
- Have a high presence of sector actors
- High frequency of economic activities

Based on the SME assessment plan, 7 key economic districts of Bangladesh were identified as part of the awareness campaign: Dhaka, Chattogram, Cox's Bazar, Gazipur, Narayanganj, Bogura, and Jashore. The sectors present in each location have been bucketed into 5 major sectors: Restaurants and Hospitality (Restaurants, Hotels, Tourism), Retail and Trade (Trade and retail, E-commerce, F-commerce), Manufacturing and Industry (RMG, Light Engineering, Furniture, Leather goods, Plastic), Agriculture and Food Production (Agriculture, Food processing, Agro-Processing), and Professional Services (ICT services).

The following table summarizes the objectives of the campaign against the selected 7 districts for the awareness campaign and the targeted prominent MSME sectors in each location:

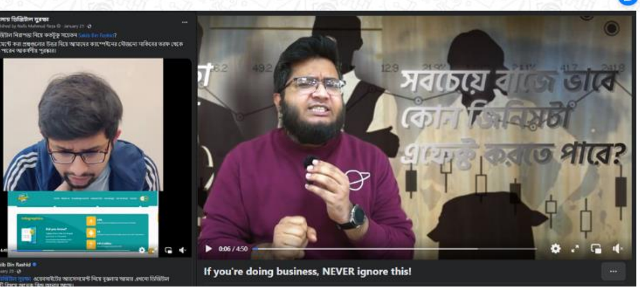
Table 1: Campaign Objectives, Locations, and Sectors

Objectives	Geographic Scope (Districts)	Targeted Sectors
1) To create awareness and induce behavior change among MSMEs regarding their Cybersecurity practices to protect their Business and Assets 2) Generate KAP (knowledge, attitude, practice) level change among MSME users and non-users of online channels 3) Preference of MSMEs for core campaign message, campaign visual colors, dissemination channels, and partnership activities	Dhaka	ICT, e-commerce, Furniture, Light Engineering, Restaurant, Service, Plastic, Traders, Construction
	Narayanganj	RMG, Service, Basic manufacturing
	Gazipur	Furniture, Workshop, foundry, bags/shoes, Retailers
	Chattogram	ICT, e-commerce, Furniture, Light Engineering, Restaurant, Retail
	Cox's Bazar	Tourism, Agro, hospitality
	Bogura	Agro, Light engineering
	Jashore	Agro, food processing

ব্যবসায় ডিজিটাল সুরক্ষা

29K likes • 29K followers

ব্যবসায় ডিজিটাল সুরক্ষা
USAID
Edit cover photo
Advertise
Manage
Edit
Home About Us Knowledge Center Assessment Campaign Get involved Policies



If you're doing business, NEVER ignore this!

2.0 Campaign Activity Report

2.1 Campaign Strategy Summary

Target Group Characteristics

The Campaign was broken into two primary activity paradigms, "Online" and Offline," based on the selected target groups that were to be reached by this campaign. The Target Groups of the campaign were defined based on the following characteristic differences –

Table 2: Characteristics of Target Groups

Serial Number.	Characteristics	Target Groups	
		Laggards	Ardent Adopters
1	**Geographic Presence**	**Area:** Peri-urban, Rural **Relevant Districts within Scope:** Faridpur, Jessore, Bogura, Cox's Bazar, Chattogram	**Area:** Urban, Peri-urban **Relevant Districts within Scope:** Dhaka, Chattogram, Narayanganj, Khulna
2	**Nature of Business/Sector**	Offline Grocers/Mom & Pop stores, Agro-machinery Manufacturing, Agriculture, Food Processing, Light Engineering, Furniture, Plastic	Restaurants, Hotels, Tourism, Trade and retail, E-commerce, F-commerce, RMG, Furniture, Leather Goods, ICT Services, Food Processing
3	**Digital Literacy**	**Low:** Minimal utilization of digital devices, connected to Facebook	**Moderate:** Frequently uses one or more digital devices for business operations,

		selling groups or as e-commerce reseller through help from Fnf but does not know how to operate themselves	operates as a f-commerce or e-commerce.
4	**Age Group**	35+ Years	20 – 35 Years
5	**Commonly Used Business Operation Platforms**	Physical Store, Facebook Page, e-commerce reseller, FMCG Supplier	Facebook Page, e-Commerce Website, Facebook Group, Multi-platform Business (Facebook + Website ++)
6	**Cyber Awareness**	Very Low	Moderate
7	**Cyber Preparedness**	Very Low	Low
8	**Exposure to Threats**	Moderate	Very High

As seen in the table, the two Groups have one characteristic connecting them, making them highly relevant to the project. Both target groups have a low level of cybersecurity preparedness, as discovered by the project's assessment. The assessment discovered that 62% of the MSMEs surveyed think they are not at risk of Cybersecurity attacks. This attitude gap, along with their gap in knowledge of how to address different cyber threats such as Phishing, Malware, Ransomware, page hack, payment scams, etc., creates major vulnerabilities for these businesses even though 34% of the MSMEs reported they were victims of Cyber Attacks and or someone they know has.

As both groups have major gaps in their KAP regarding Cybersecurity, Digital Hygiene, and Cyber Threats, they have been the primary focus of the campaign's messaging that emphasized messaging meant to address their knowledge gap and bring an attitude change.

Campaign Quarters

The campaign was divided into 3 quarters, each serving a different purpose in orienting the TG (Target Group) with cybersecurity awareness. Phase 1 enlightened our audience regarding the various types of cybersecurity threats that MSME owners are predominantly facing in Bangladesh, quarter 2 elaborated on protective measures and provided reassurance that these threats can be prevented, and finally, quarter 3 aimed to ensure that cybersecurity habits and internet hygiene become a greater part of the collective consciousness.

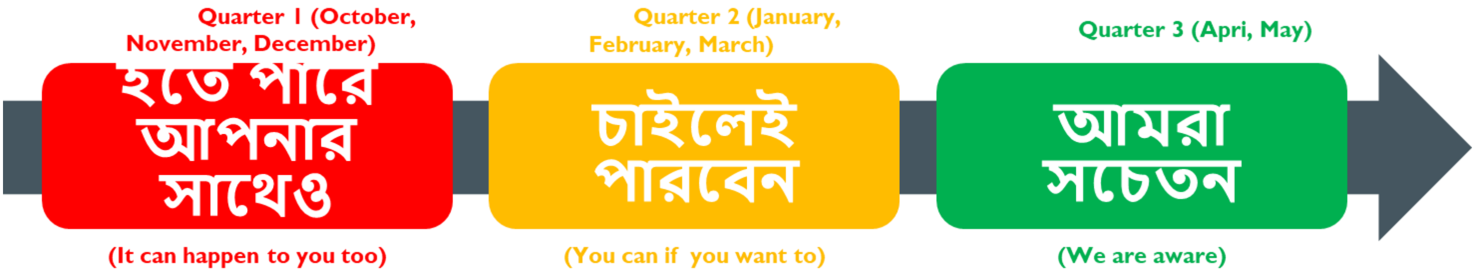

Quarter 1 (October, November, December)
হতে পারে আপনার সাথেও
(It can happen to you too)
Quarter 2 (January, February, March)
চাইলেই পারবেন
(You can if you want to)
Quarter 3 (Apri, May)
আমরা সচেতন
(We are aware)

Figure 2: Quarter core messages

Quarter 1 (October, November, December): Small and medium enterprise owners often believe that cyber-attacks only happen to large companies. They are largely unaware that it may happen to them as well. To address this, quarter 1 of the campaign enlightened MSME owners regarding various cyber threats they are exposed to, how to identify them, and how to stay safe.

Quarter 2 (January, February, March): Enterprise owners often think ensuring cybersecurity is hard and/or costly. Through various series of content, the campaign aimed to show that it is very easy and they just need to take the initiative to learn. Quarter 2 emphasized problems specific to MSME owners relying heavily on online business channels.

Quarter 3 (April, May): Enterprise owners in Bangladesh tend to follow their peers for advice and good practices. The campaign team capitalized on the beneficiaries and Key Opinion Leaders to promote Cybersecurity Awareness further to them as well. The goal of quarter 3 was to promote cybersecurity as a concept to the online business community in Bangladesh and normalize good practices among enterprise owners.

Message Approach

To ensure that the campaign messaging transitions smoothly across the campaign quarters, The campaign used the Attention, Interest, Desire, Action (AIDA) principle to ensure consistent messaging transitions across campaign quarters. The (AIDA) principle refers to a hierarchy of desired impacts similar to how customers engage with advertisements in a sales funnel.

The attention phase will capture the attention of the Target Group; the interest phase will spark the curiosity of the Target Group to look for content they can relate to. The desire phase will shift the target group's mindset from "I like this" to "I want this," finally, the action phase will convert viewers to users: The phase where the Target Group is actively engaging with the content.

The following message themes were drafted for the interest, desire, and action quarters. These messages have been selected to create and raise interest among the viewers. These messages were crafted to generate interest among the audience, allowing the campaign to build momentum.

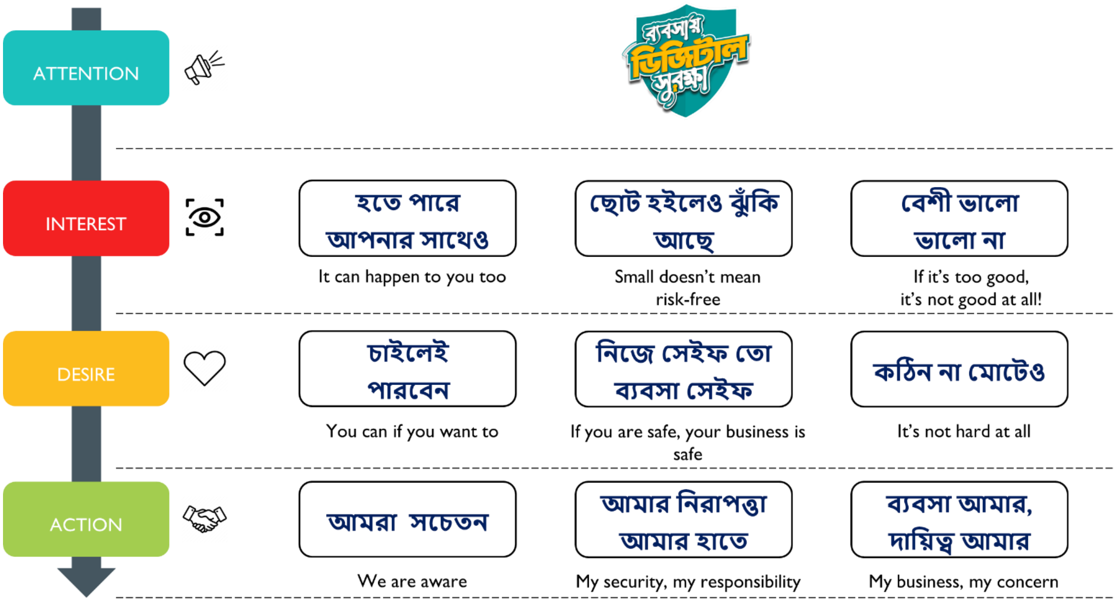


Figure 3: Key Campaign Messages

Partnerships

For the two MSME target groups selected, both are prone to putting more significance on Brand recognition and the organization's public reputation when accepting any messaging shown to them through social media or disseminated among them through workshops and theater performances; for example, for MSME owners in Bangladesh, a message coming from the government would be seen as more reliable and trustworthy.

Partnerships will be leveraged in this regard to ensure:

1) The campaign messages are amplified and vetted by stakeholders that are relevant to the TG (through collaboration with important ecosystem actors: government agencies and industry associations)

2) The campaign messages are disseminated in the relevant channels (through partnerships with private sector actors that work closely with large MSME populations: B2B service providers, on-demand service providers, and e-commerce platforms)
3) The campaign activities can ensure the presence of relevant TG through accessing partner networks of MSMEs across target districts

2.2 Overview of Campaign Activities

The "Bebshay Digital Shurokkha" Campaign was developed as an awareness campaign on Digital Safety, Cybersecurity, and Mis/dis-information that was aimed at the Micro, Small, and Medium Enterprises of Bangladesh that have already stepped into the online marketplace or are soon to embark on that journey due to the potential of exponential growth in the online platforms and marketplaces. The campaign was developed with three primary activity streams, and one additional activity stream was introduced in quarter 2.

Online Media Campaign

The campaign ran a social media campaign that reached 3.4 million people with multiple interconnected contents utilizing various high conversion channels to achieve the campaign goals to generate reach and engagement with the target audience and develop a catalog of learning snippets and contents that would be helpful for the target group in improving their Digital Hygiene. The online campaign ran in conjunction with the Campaign Website, which carried two major components, including Knowledge material regarding specific Cyber Threats, Campaign Activity Promotion, and, most importantly, a Cybersecurity Assessment Test designed for the MSME cohort selected for the campaign, which has received over 3000 responses to gauge their change in Cybersecurity Awareness and Preparedness throughout the campaign. We collaborated with influencers, including Sakib Bin Rashid[3] from 10 Minute School and Nafees Salim[4].

Offline Activation Campaign

The offline activation effort was designed to generate a more meaningful impact on a measured segment of the core target group. The activities included ten mobile activation units on MSME Fairs and MSME-focused events, 3 Interactive Community Theaters, and the featured activity was the 12 Cybersecurity Awareness Workshop. The mobile activation aimed to directly connect with communities of MSMEs in different district clusters and reach the peri-urban MSMEs not as deeply connected with the online business space. In contrast, the workshops aimed to create a lasting impact and impart cyber awareness, cyber preparedness, the process of incident response, and specific cyber threats such as Malware, Ransomware, Phishing, Hacking, and more. The workshop's objective was to build the capacity of the MSMEs to keep themselves secure and be prepared to act in case of an incident.

Partnership Establishment

One of the most important preparatory parts of the campaign was important in successfully executing all the activities. Most of the offline activations and some of the online campaign runs involved collaboration with relevant Stakeholders in the MSME sector and Influencers. Our partnership and collaboration efforts aimed to connect relevant Government Entities, MSME Communities, Associations, and Private Sector Stakeholders with our activities to improve their effectiveness and assist MSMEs connected with these organizations to connect with our activities for their benefit. The collaborations have allowed the campaign to further its reach, organize more events, and, most importantly, connect with active MSMEs from all over Bangladesh. The campaign connected with a2i, SME Foundation, Women and E-commerce, e-CAB, BdOSN, Bank Asia, and the BRAC Bank[5].

Cybersecurity Support Center for MSMEs (OSD)

[3] (Sakib Bin Rashid, n.d.)
[4] (Nafees Salim, n.d.)
[5] (BRAC Bank, n.d.)

Beyond the planned activities, in part due to partnerships achieved during the campaign and the MSMEs the campaign has connected with, it has brought about the development of additional campaign activity. The MSMEs engaging with the campaign's activities started gradually reaching out to the campaign regarding their Cybersecurity issues and Cyber Incidents. We also received multiple requests from MSMEs for us to investigate the issues they are facing during our workshops. The additional activity, a Cybersecurity Support Center pilot run, was incorporated into the campaign. The support center assisted MSMEs with their business and personal hygiene Cybersecurity Setup and assisted them with working with law enforcement to expedite their reported Cyber Crime cases. The support center launched in the middle of the campaign's second quarter solved 24 cases, and received 30 incident reports. Beyond that, over 400 Cybersecurity-related queries have been addressed as part of the scope of the support center, which includes assisting MSMEs with turning on their MFA, setting up backup accounts, and more.

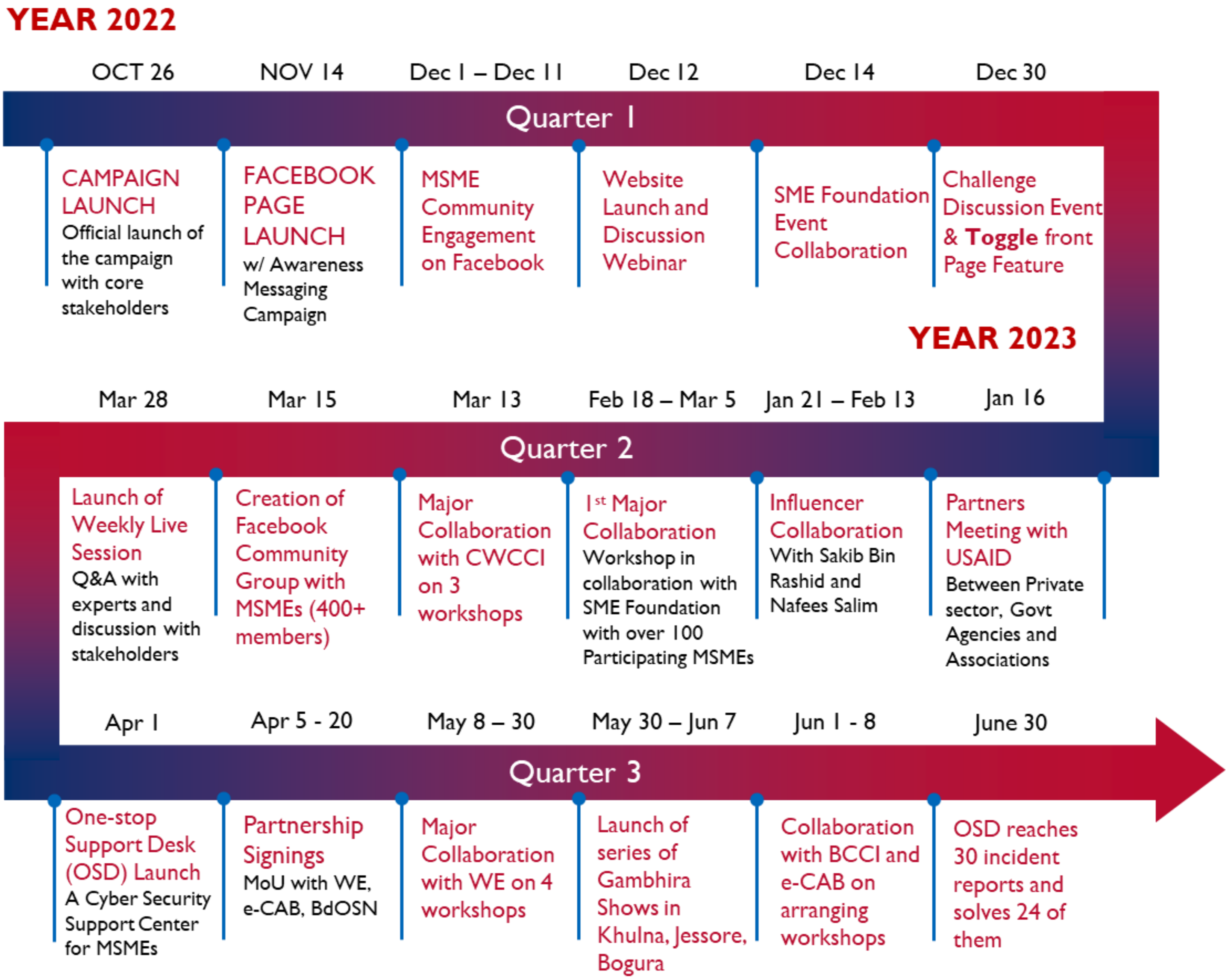
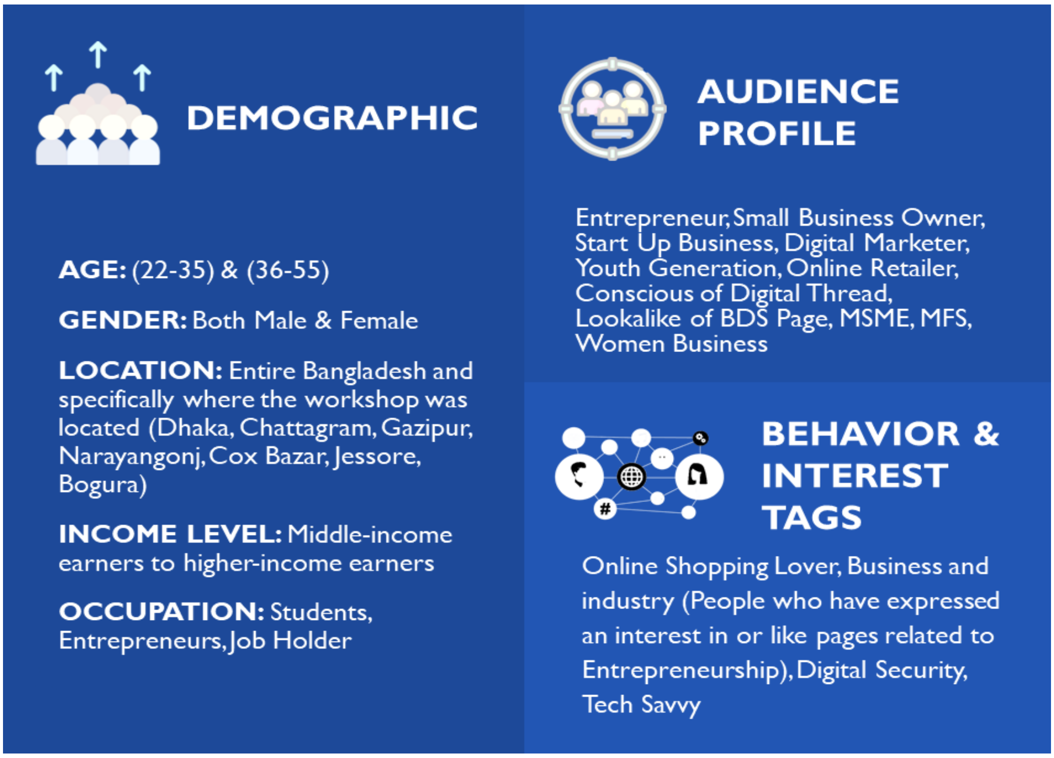

YEAR 2022
OCT 26
NOV 14
Dec 1 – Dec 11
Dec 12
Dec 14
Dec 30
Quarter 1
CAMPAIGN LAUNCH Official launch of the campaign with core stakeholders
FACEBOOK PAGE LAUNCH w/ Awareness Messaging Campaign
MSME Community Engagement on Facebook
Website Launch and Discussion Webinar
SME Foundation Event Collaboration
Challenge Discussion Event & Toggle front Page Feature
YEAR 2023
Mar 28
Mar 15
Mar 13
Feb 18 – Mar 5
Jan 21 – Feb 13
Jan 16
Quarter 2
Launch of Weekly Live Session Q&A with experts and discussion with stakeholders
Creation of Facebook Community Group with MSMEs (400+ members)
Major Collaboration with CWCCI on 3 workshops
1st Major Collaboration Workshop in collaboration with SME Foundation with over 100 Participating MSMEs
Influencer Collaboration With Sakib Bin Rashid and Nafees Salim
Partners Meeting with USAID Between Private sector, Govt Agencies and Associations
Apr 1
Apr 5 - 20
May 8 – 30
May 30 – Jun 7
Jun 1 - 8
June 30
Quarter 3
One-stop Support Desk (OSD) Launch A Cyber Security Support Center for MSMEs
Partnership Signings MoU with WE, e-CAB, BdOSN
Major Collaboration with WE on 4 workshops
Launch of series of Gambhira Shows in Khulna, Jessore, Bogura
Collaboration with BCCI and e-CAB on arranging workshops
OSD reaches 30 incident reports and solves 24 of them

Figure 4: Roadmap of Phase 1

Quarter 1 Objectives:



DEMOGRAPHIC

AGE: (22-35) & (36-55)

GENDER: Both Male & Female

LOCATION: Entire Bangladesh and specifically where the workshop was located (Dhaka, Chattagram, Gazipur, Narayangonj, Cox Bazar, Jessore, Bogura)

INCOME LEVEL: Middle-income earners to higher-income earners

OCCUPATION: Students, Entrepreneurs, Job Holder

AUDIENCE PROFILE

Entrepreneur, Small Business Owner, Start Up Business, Digital Marketer, Youth Generation, Online Retailer, Conscious of Digital Thread, Lookalike of BDS Page, MSME, MFS, Women Business

BEHAVIOR & INTEREST TAGS

Online Shopping Lover, Business and industry (People who have expressed an interest in or like pages related to Entrepreneurship), Digital Security, Tech Savvy

Figure 5: Quarter 1 demographic, audience, and behavior tag

The first quarter had the following key objectives to set the basis for the rest of the campaign. They are as follows –

a. Generate change in the "Knowledge" based indicators of the KAP indicators from the baseline assessment on MSMEs of the project through awareness-based content campaigning.
b. Launch and promote the campaign website along with a self-assessment test on cybersecurity to gauge the campaign audience's initial level of cybersecurity preparedness for their business.
c. Garner interest from key stakeholders in the MSME sector, including Government Agencies, Private Sector Organizations, Financial Institutions, Business Associations, and MSME Communities to enable partnership and collaboration opportunities.

Quarter 2 Objectives:

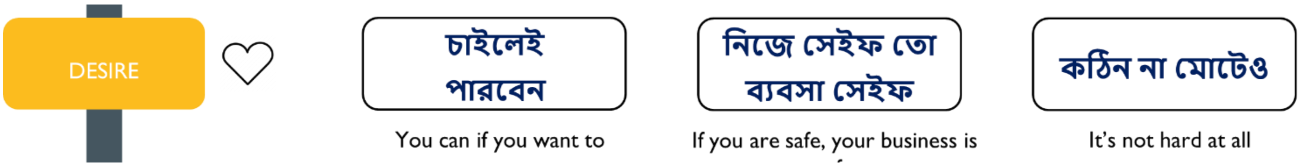


Figure 6: Desire key messages

The key campaign activations were slated for the second and featured quarter of the campaign. This quarter started the primary campaign activities contributing to the campaign goals.

The objectives for this quarter were as follows-

a. Generate change in the "Knowledge" and "Attitude" based indicators of the KAP indicators from the Baseline assessment on MSMEs of the project through a combination of contents on specific cyber threat awareness, preventative measures, and to-dos to tackle them.

b. Initiate collaborations and partnerships with relevant stakeholders to proliferate campaign messages and distribute important resources to the target groups.
c. Execute prime campaign activities such as collaborative events and cybersecurity workshops to build a measured number of MSMEs' cybersecurity preparedness for their business and personal cyber safety.
d. Preliminarily analyze the campaign's effectiveness in achieving the goal and impact on the campaign activities' direct beneficiaries to understand the grassroots-level concerns of MSMEs.

Quarter 3 Objectives:

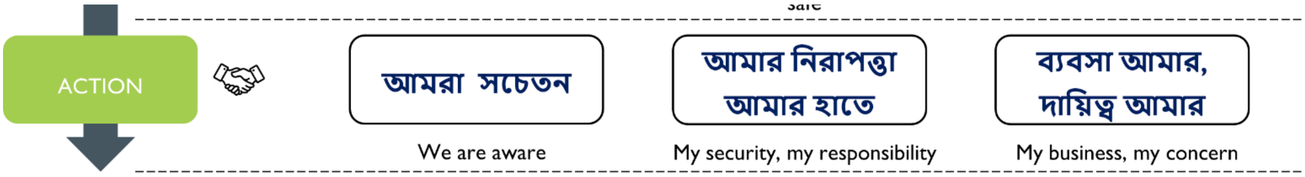


Figure 7: Action key messages

As the campaign reaches its apex, the goal is to ensure it reaches the project's target objective. The third quarter saw the completion of capacity-building workshops and offline activations such as the Cybersecurity board game and the Interactive Community theaters. The specific objective of the third quarter is as follows –

a. Publish campaign content focused on generating change in the “Practice” based indicators of the KAP indicators from the Baseline assessment on MSMEs of the project through a combination of contents on specific cyber threat awareness, preventative measures, and to-dos to tackle them.
b. Further, secure partnerships with key stakeholders and execute joint campaign activities.
c. Complete the core activities of the campaign, including all workshops, mobile activations, and other offline activities.
d. Conclude the OSD Support Center's piloting and develop a showcase for the pilot program results.
e. Conduct a final run of the self-assessment test among the beneficiaries to measure the change in cybersecurity preparedness.

3.0 Breakdown of Campaign Achievements

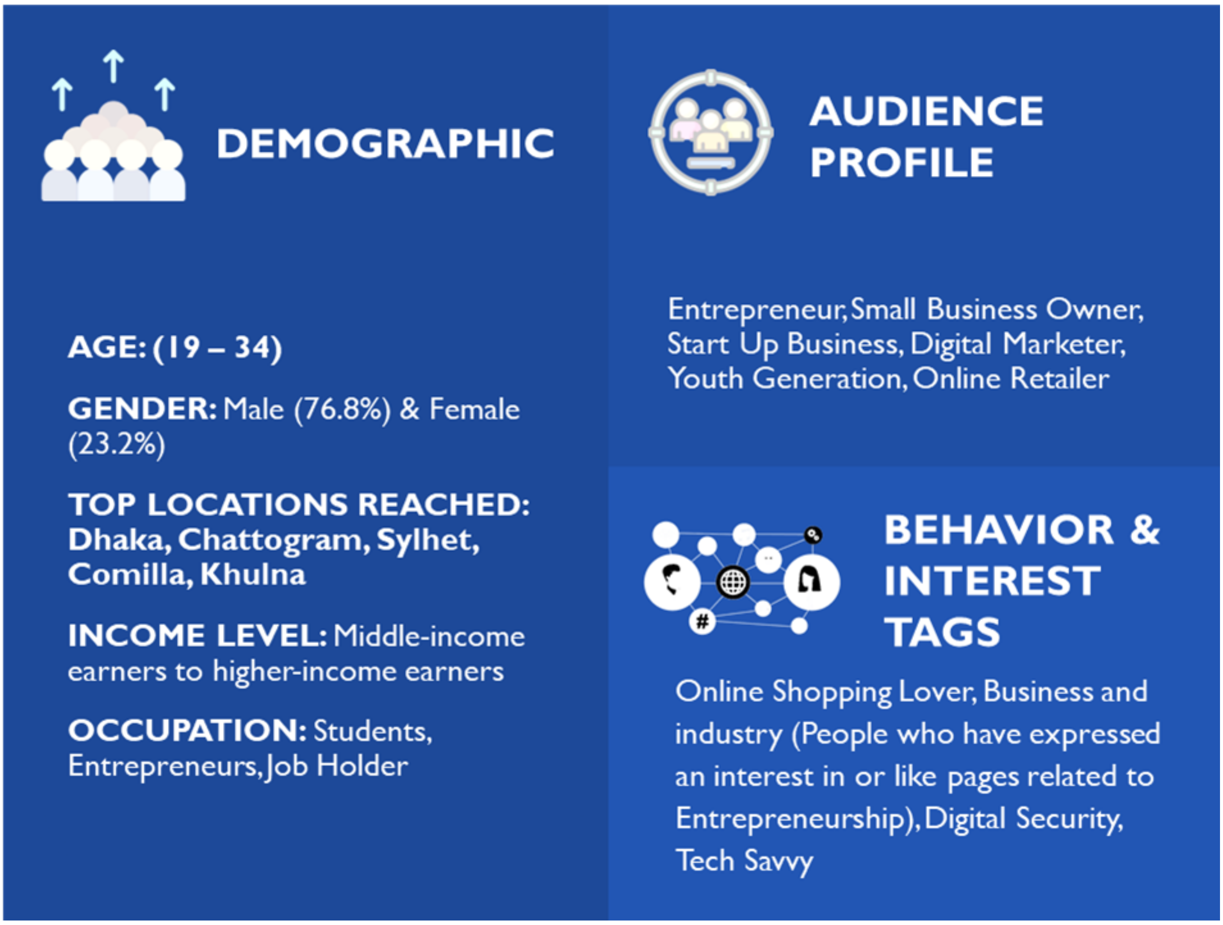
3.1 Online Campaign Achievements

The campaign's digital presence had two primary channels: the social media platform Facebook and the campaign website. The website acted as the hub for the campaign's online presence. At the same time, the Facebook page was set up to engage the audience with cybersecurity-focused content and channel them to the website for more content and a cybersecurity assessment test. However, social media had several functions beyond this, which will be discussed in the following section.

3.1.1 Online Activities Overview

The first quarter of the campaign primarily focused on launching the campaign's **Facebook page**[6] and **website, sharing awareness-based content among the project's geographic cohorts**. The campaign reached a significant number of audiences belonging to the following characteristics:

Quarter I Audience Characteristics Results



DEMOGRAPHIC

AGE: (19 – 34)

GENDER: Male (76.8%) & Female (23.2%)

TOP LOCATIONS REACHED: Dhaka, Chattogram, Sylhet, Comilla, Khulna

INCOME LEVEL: Middle-income earners to higher-income earners

OCCUPATION: Students, Entrepreneurs, Job Holder

AUDIENCE PROFILE

Entrepreneur, Small Business Owner, Start Up Business, Digital Marketer, Youth Generation, Online Retailer

BEHAVIOR & INTEREST TAGS

Online Shopping Lover, Business and industry (People who have expressed an interest in or like pages related to Entrepreneurship), Digital Security, Tech Savvy

The social media campaign had multiple content streams planned to include three distinct quarters to consider the KAP (Knowledge, Attitude, Practice) framework set for the campaign.

Small and medium enterprise owners often believe that cyber-attacks only happen to large companies. They

[6] https://www.facebook.com/msmedigitalsafety

are largely unaware that it may happen to them as well. To address this, Quarter 1 of the campaign informed MSME owners regarding various cyber threats they are exposed to, how to identify them, and how to stay safe.

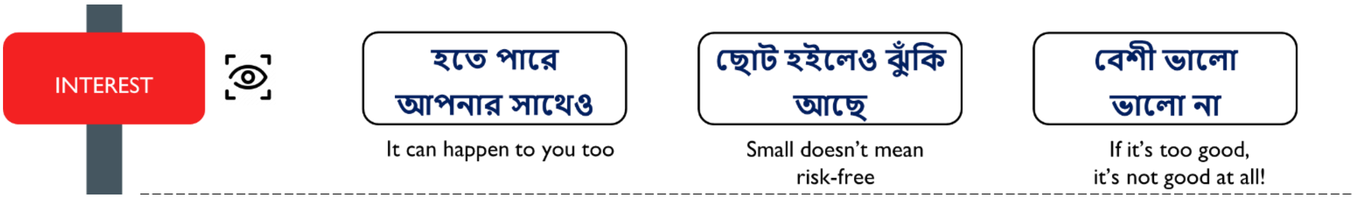


Figure 8: Interest key messages

The first quarter of the campaign had content focused on awareness messaging on the most common Cyber Threats and aimed to create recognition among the target groups regarding the most common cyber threats to prepare them for the messages of the second quarter.

The topics of focus were –

1. Malware
2. Phishing Scam
3. Ransomware
4. Insider Threats
5. Online Supplier Scam
6. Business page hacking and page fraud
7. Fake delivery or fake address scam
8. Fake payment

The overall objectives of the online activities were to launch the campaign and its primary online components, which included –

1. Awareness Messaging Content
2. Launch of the Campaign Website
3. Promotion of the Cybersecurity Assessment Test
4. Garnering attention from the key stakeholders for potential partnerships

To focus on the MSME owners who have been reached and engaged with the different content and activities to create awareness about the most common Cyber Threats and real-life cases of Cyber incidents, the second quarter focused on empowering the MSMEs by launching the social media campaign **"You can if you Want to"** emphasizing Enterprise owner themselves can protect their Online Business and Digital Assets. The focus of this quarter was to introduce the practices and tools available to them to secure their online business. As such, this collection of content focused on inspiring MSMEs to reach out and impact their attitude toward the security of their businesses.

The final quarter of the campaign focused on completing the planned online campaigns to promote the newly added OSD and another push for the followers and project beneficiaries to take the self-assessment test on the campaign website. Enterprise owners in Bangladesh tend to follow their peers for advice and good practices. The campaign team capitalized on the beneficiaries and Key Opinion Leaders to promote Cybersecurity Awareness further to them as well.

The campaign, completing two-thirds of its timeline, had reached its initial goals for the online activation. As per the online campaign plan, the contents for the third quarter were aimed at having MSMEs take "Action." In addition to that, the different components introduced during the activation, both planned and improvised, should be operating to reach their objectives.

The last quarter of the campaign will focus on the following online activities –

1. Social media content showcasing countermeasures to cyber-attacks.

2. Strengthening the campaign community group with weekly Q&A and frequent postings to generate engagement.
3. Promotion of OSD to ensure effective piloting of the service.
4. Re-emergence of the Self-assessment test to gauge changes in average scores of the campaign followers and beneficiaries

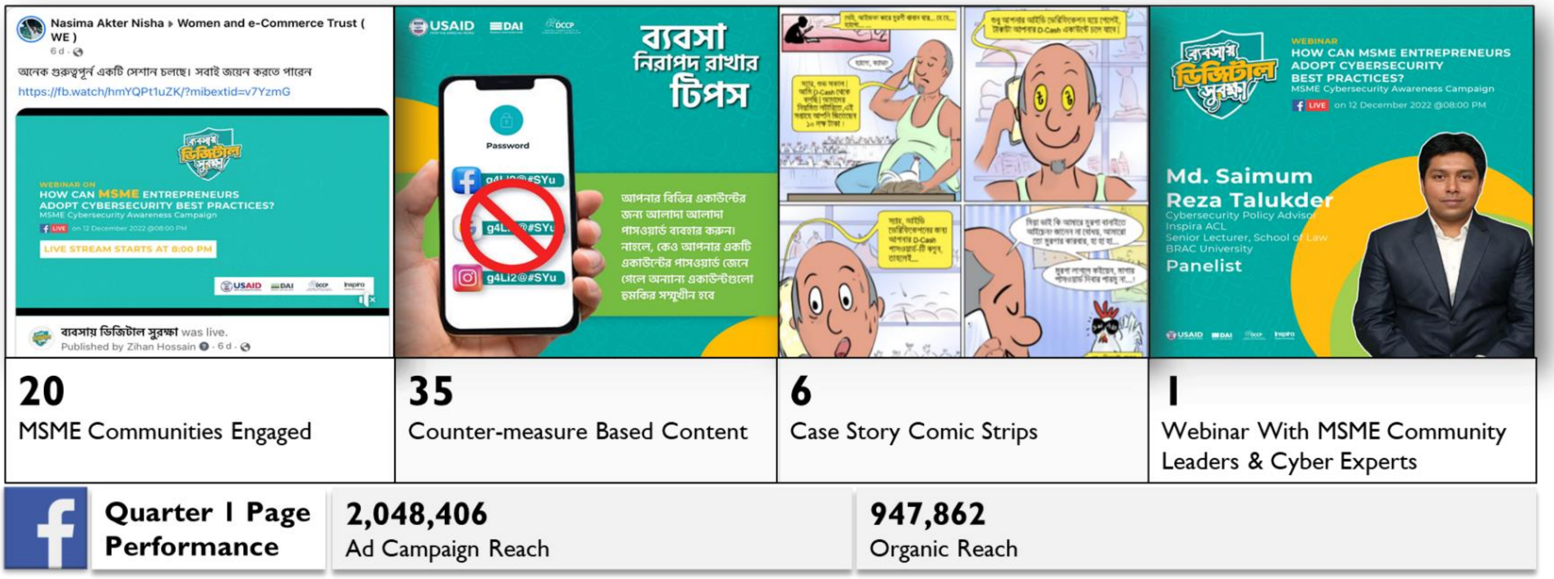

Nasima Akter Nisha ▸ Women and e-Commerce Trust (WE)
https://fb.watch/hmYQPt1uZK/?mibextid=v7YzmG
HOW CAN MSME ENTREPRENEURS ADOPT CYBERSECURITY BEST PRACTICES?
LIVE STREAM STARTS AT 8:00 PM
ব্যবসায় ডিজিটাল সুরক্ষা was live.
USAID
DAI
ব্যবসা নিরাপদ রাখার টিপস
Password
g4Li2@#SYu
Md. Saimum Reza Talukder
Cybersecurity Policy Advisor, Inspira ACL
Senior Lecturer, School of Law BRAC University
Panelist
20
MSME Communities Engaged
35
Counter-measure Based Content
6
Case Story Comic Strips
1
Webinar With MSME Community Leaders & Cyber Experts
Quarter 1 Page Performance
2,048,406
Ad Campaign Reach
947,862
Organic Reach

Figure 9: Quarter 1 online achievements

3.1.2 Social Media Achievements

The social media campaign had several components, all focused on working together, and the campaign's website was used to garner widespread reach and engagement with the campaign's learning components. Through the execution of these campaign components, the campaign reached over 900,000 organic reach and 70,000 engagements (like, share, comment, link click, video views) in the first quarter of the campaign, showing a positive trajectory for the page and its content. Some of the major activities included six 2D Comic strips that depicted real-life stories from respondents from the Assessment phase of the project. On May 1st, 2023, a highly engaging webinar was held titled "Digital Safety in Business: Women's Perspective," which garnered over 13,000 organic reach and 1000+ comments and questions for the panel[7]. The panelists included notable MSME and Cybersecurity experts:

- Nasima Akter Nisha (Managing Director of Women and e-Commerce Forum and Secretary of e-CAB)
- Tanvir Hassan Zoha (Assistant Professor, Department of Computer Science and Engineering, Bangladesh University of Business and Technology
- Md. Saimum Reza Talukder (Senior Lecturer, School of Law, BRAC University)

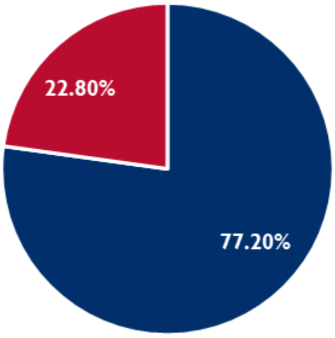


Figure 10 Facebook audience gender distribution

[7] (Women in e-Commerce, n.d.)

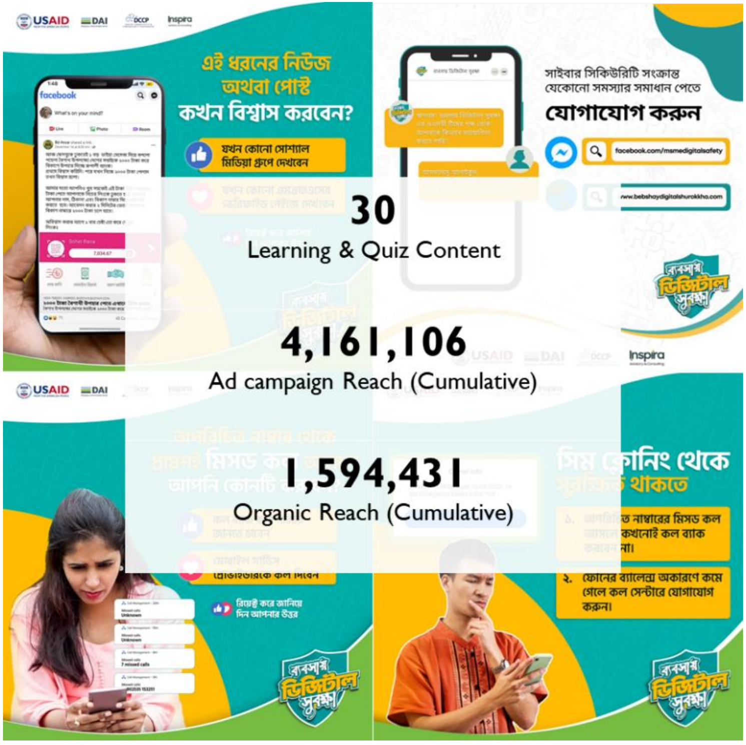
- Irin Parveen (Executive Director, Women and e-Commerce Forum)

The results indicate a high level of interest among the target group. Specifically, the contents gained most of the attention from the Ardent Adopter target group based on Dhaka, Chattogram, and Sylhet. According to insights extracted from the campaign's Facebook page. 35% of the audience was in Dhaka, and Chattogram was leading behind Dhaka at 10%.

The social media campaign's primary focus was on the Ardent Adopters, and in Quarter 1, the targeting parameters proved effective at reaching the members of this group. However, of the social media users who saw and interacted with the campaign content,77.2% were male, and 22.8% were female. This indicates that the target parameters need adjustments for more female MSMEs entering Quarter 2.

Therefore, in Quarter 2, the social media content aimed to build on the awareness-based campaigning efforts from Quarter 1 by introducing tools and methods that the audience could use to improve their online businesses' cybersecurity and digital hygiene. A key Quarter 2 campaign objective was to improve the target audiences' scores on the "Attitude" KAP indicator. Campaign content designed to achieve this objective included:

1. **Learning and Quiz Content:** On the Facebook page, we posted quick interactive quizzes for the audience to vote on securing their personal and business profiles, Two-factor authentication, identifying certain cyber threats, reporting certain cyber incidents, advanced ID recovery methods, and more. This was made possible by developing content for social media and the website, where the website learning content is specific.



USAID
DAI
DCCP
Inspira
এই ধরনের নিউজ অথবা পোস্ট কখন বিশ্বাস করবেন?
সাইবার সিকিউরিটি সংক্রান্ত যেকোনো সমস্যার সমাধান পেতে
যোগাযোগ করুন
facebook.com/msmedigitalsafety
www.bebshaydigitalshurokkha.com
30
Learning & Quiz Content
4,161,106
Ad campaign Reach (Cumulative)
1,594,431
Organic Reach (Cumulative)
সিম ক্লোনিং থেকে

Figure 11: Website achievements

The campaign strategy followed the KAP model to develop content packages for each cyber threat. During Quarter 2 of the campaign, the Knowledge and Attitude part of the package for each cyber threat type was deployed.

This quarter focused on steps and actions MSMEs can take to protect their business and personal digital assets from the cyber threats mentioned and defined in the first quarter of the project. The messaging focused on content regarding the following cybersecurity tools –

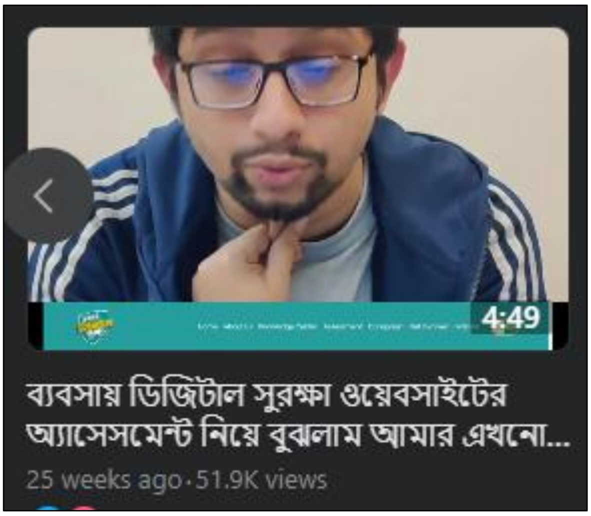
a. Two-factor Authentication
b. How to identify phishing links
c. What to do if a mobile operator asks for sensitive data
d. How to avoid fake delivery scams
e. How to identify payment scams
f. How to set a strong password

2. **Influencer Collaboration:**

One of the most effective options to generate a large surge of organic reach and engagement is collaborating with online content creators and influencers with an audience relevant to the campaign. They will usually have a large following of real individuals and minimal concerns regarding bots that may be present in the engagement and reach metrics. To that end, the campaign collaborated with 3 content creators who are intrinsically connected with the MSME community of Bangladesh and are well-known figures nationwide. Our collaboration efforts went as follows –

a. **Self-Assessment Test Promotion with Sakib Bin Rashid:**
This collaboration was determined with Sakib Bin Rashid due to his large following on Facebook, which was our primary communication medium. Sakib Bin Rashid also has a large following of MSMEs for the tips and tricks videos he will post regarding running certain operations on Facebook, introducing new mechanics to his large audience.
To that end, we devised a video promotion where Sakib Bin Rashid takes the Self-assessment test to see if he is cyber-safe.

Synopsis: Sakib Bin Rashid takes the cybersecurity Self-Assessment Test and realizes that even he does not know how to manage several scenarios presented in the assessment Test. As he learns about these Cyber Threats, he urges his audience to also take the self-assessment test to learn about their understanding of cybersecurity and share their score in the Comment section.



ব্যবসায় ডিজিটাল সুরক্ষা ওয়েবসাইটের অ্যাসেসমেন্ট নিয়ে বুঝলাম আমার এখনো...
25 weeks ago · 51.9K views

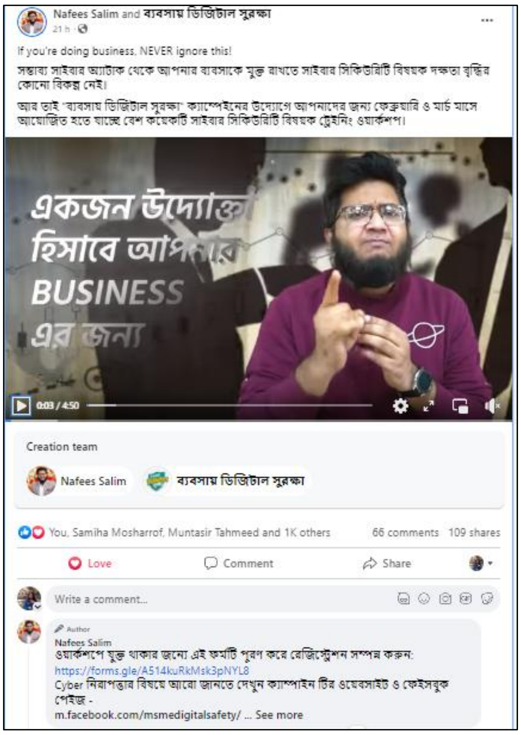
Figure 12 Snapshot of Sakib Bin Rashid video

Outcome: The video managed to get 51,900 views and 100+ comments/responses. In addition, the website assessment test on the day the video was published got approximately 200 new assessment test submissions.

b. **Promotion of the MSME Cybersecurity Workshop with Nafees Salim:** As the second quarter also saw the kick-off of the activation planned for the workshop, it was a good opportunity to promote the campaign to the mass audience through collaboration with a well-known figure in the MSME community of Bangladesh. Nafees Salim is a content creator and podcaster who focuses his content on business operations, tips, news, and discussions around MSME businesses and their growth. He is a respected figure in the MSME sector, especially among young entrepreneurs.

Synopsis: As such, the campaign collaborated with him to launch a video to talk about the importance of Cybersecurity for MSMEs in their business operations and encourage them to register for the MSME cybersecurity Workshop arranged by the campaign.

Outcome: The video reached 30,000 views on Facebook, 1,500 likes, 76 Comments, and 109 shares. This indicated that people watched the


Nafees Salim and ব্যবসায় ডিজিটাল সুরক্ষা
21 h

If you're doing business, NEVER ignore this!

সম্ভাব্য সাইবার অ্যাটাক থেকে আপনার ব্যবসাকে মুক্ত রাখতে সাইবার সিকিউরিটি বিষয়ক দক্ষতা বৃদ্ধির কোনো বিকল্প নেই।

আর তাই "ব্যবসায় ডিজিটাল সুরক্ষা" ক্যাম্পেইনের উদ্যোগে আপনাদের জন্য ফেব্রুয়ারি ও মার্চ মাসে আয়োজিত হতে যাচ্ছে বেশ কয়েকটি সাইবার সিকিউরিটি বিষয়ক ট্রেইনিং ওয়ার্কশপ।

Creation team
Nafees Salim ব্যবসায় ডিজিটাল সুরক্ষা

You, Samiha Mosharrof, Muntasir Tahmeed and 1K others 66 comments 109 shares

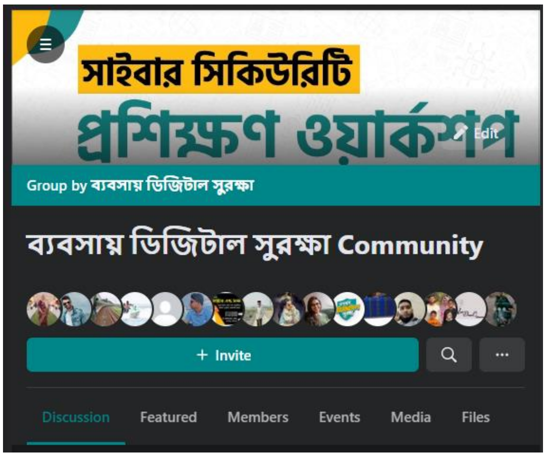
Author
Nafees Salim
ওয়ার্কশপে যুক্ত থাকার জন্যে এই ফর্মটি পুরণ করে রেজিস্ট্রেশন সম্পন্ন করুন:
https://forms.gle/A514kuRkMsk3pNYL8
Cyber নিরাপত্তার বিষয়ে আরো জানতে দেখুন ক্যাম্পাইন টির ওয়েবসাইট ও ফেইসবুক পেইজ -
m.facebook.com/msmedigitalsafety/ ... See more

Figure 13 Snapshot of Nafees Salim video

content, engaged, and found it useful enough to share. We received 210 registrations from interested MSME participants who want to take the workshop directly because of that video.

3. **Facebook Cybersecurity Discussion Community:**

The "Bebshay Digital Shurokkha" campaign during its first quarter attracted a lot of followers interested in learning more and discussing and asking questions about cybersecurity that they had. During the second quarter, the number of messages sent to the Facebook page inbox grew rapidly. In addition, the other online and offline activities were creating a following that needed a two-way communication channel that would allow them to share their thoughts and questions regarding cyber threats and incidents that have occurred. To provide these motivated MSMEs a platform to learn more about cybersecurity, reach out to the campaign team directly, and share their stories, the campaign page launched the "Bebshay Digital Shurokkha Community" on Facebook[8]. During quarter 2, the community had 215 active MSMEs as members.



সাইবার সিকিউরিটি প্রশিক্ষণ ওয়ার্কশপ

Group by ব্যবসায় ডিজিটাল সুরক্ষা

ব্যবসায় ডিজিটাল সুরক্ষা Community

Figure 14 Facebook cybersecurity group

The campaign team moderated the community. It was made to be a learning platform and a discussion forum for MSMEs interested in knowing more about Cybersecurity that would help protect their businesses. The community moderator posted 2 to 3 daily learning and engagement content, discussion, and help posts.

4. **Live Q&A Session with Cybersecurity Experts (Pilot):**

During the second half of Quarter 2 of the campaign, while both online campaign and offline activities such as the workshops and MSME Fair mobile activations were running, we received requests from many MSMEs participating in events and commenting on posts that they were not able either join workshops due to their busy schedule or they have more questions that they would like the campaign to respond to. The campaign team thus adapted to the needs of the beneficiaries and started a weekly Live Q&A session led by the Cybersecurity Experts part of the campaign to answer pressing questions and discuss specific Cyber threats or digital hygiene practices in more detail.

The first pilot session in the community group saw 40 plus concurrent viewers, 55 peak viewers live, and 37 queries from audiences on the cyber threat discussed in the session. The feedback has been very positive, and people have shared positive remarks and a calling for more sessions with more people.

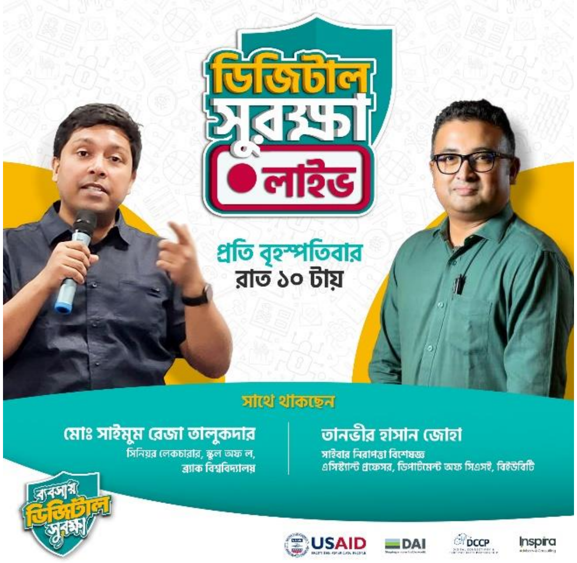


Figure 15: live Q&A session

The third quarter of the social media campaign focuses on content that showcases the different countermeasures that MSMEs can take to secure their business from cyber-attacks. The content strategy involved a reiteration of relevant cases through short comic strips to create recall among the audience using the most effective medium discovered during the earlier quarters.

[8] (Bebshay Digital Shurokkha, n.d.)

This method was used throughout the quarter, focusing on the most common cyber threats: Malware, Ransomware, Phishing, and Insider Threats. The content created for this purpose was especially effective according to the metrics, as each comic strip reached over 1000 likes and 20 to 50 comments, and the countermeasure content also saw increased engagement. Particularly the audio-visual content, each has approximately 8,000 to 10,000 views.

Beyond that, the campaign's social media also featured the following content –

1. **Webinar in collaboration with Women and E-commerce Trust on "Women's perspective on MSME Cybersecurity."**
   Cyber harassment, bullying, identity theft, and personal information breaches are threats women in Bangladesh and women entrepreneurs in Bangladesh commonly face. We recorded multiple cases that women entrepreneurs shared during the campaign activities. Thus, in collaboration with the largest women's MSME community, the campaign arranged a webinar to bring the challenges women face to the forefront and address some tactics that can help women be more resilient to cyberattacks.
   The webinar was arranged for Mayday 2023 and garnered a large MSME audience. The webinar had over 300 concurrent viewers and cumulatively had 13,000 views, 1,500 comments, and questions from MSMEs who joined live.

2. **Influencer collaboration with Smita Chowdhury**
   The campaign worked with social media influencer Smita Chowdhury to produce a video titled "Are Local MSMEs Cyber Aware? Smita Chowdhury Quizzes local Fair MSMEs on Cybersecurity."
   The objective of the video: To conduct impromptu interviews of MSMEs participating in the Sowda Hut MSME Fair to engage them and gauge their cybersecurity knowledge. Smitha Chowdhury presented a 5-question quiz to the participating MSME, and any MSMEs scoring 4 or more were gifted with a cybersecurity-themed "Snakes and Ladders" game board.
   The initiative added to the promotion of the campaign on digital platforms through a vlog of the activity posted by the influencer Smitha Chowdhury on her Facebook page, which has over 500,000 followers.

   We engaged over 50 MSMEs and quizzed 10 MSMEs, and the video had over 32,000 views on Facebook[9].

3. **Weekly Live Q&A Session with Cybersecurity Experts**

Throughout the campaign, during workshops, MSMEs have expressed a range of questions regarding their personal and business-related cybersecurity to the trainers and the Campaign Team. To address these questions further and engage with the MSMEs on a broader scale, 4 additional Facebook Live Q&A sessions with the trainers and, in some instances, in collaboration with partners were conducted.

3.1.3 Campaign Website Achievements

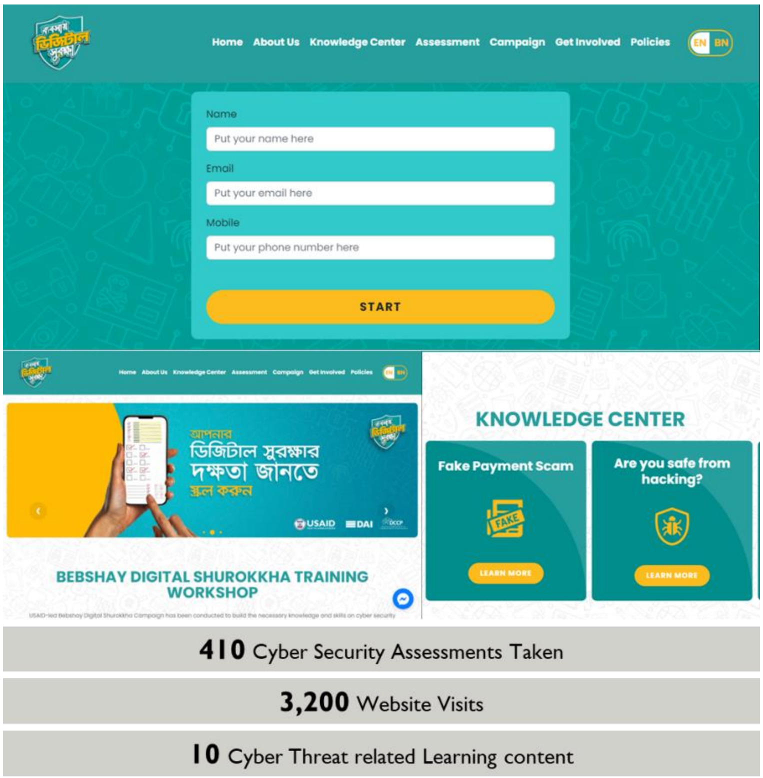
Phase 1 also launched the Campaign website alongside the webinar. The launch featured a promotional video showcase of the website. Several contents were developed linking back to the website, specifically, the assessment test, to find relevant participants from the target group yet to be exposed to the information shared through the campaign to participate.
The website consisted of two key components –

[9] https://www.facebook.com/letsknowwithsmita/videos/988593252565883

1. Knowledge Articles on Cyber Threats

The campaign website was populated with useful articles that explain Cyber Threats, how to identify them, what steps to take as a precaution against them, and what steps to take when facing a particular cyber threat. The articles also worked as a downloadable resource, allowing MSMEs to read up on them at their leisure and even print them out to use as teaching material for themselves and their employees. The first quarter covered 10 such Cyber threats that are most common in Bangladesh and especially among MSMEs in Bangladesh –

A. Malware
B. Ransomware
C. Phishing Scam
D. Insider Threat
E. Fake Delivery
F. Fake Payment
G. Supplier Scam
H. Facebook Hack
I. Gmail Recovery
J. Business ID lockout



410 Cyber Security Assessments Taken

3,200 Website Visits

10 Cyber Threat related Learning content

Figure 16: Website articles

Each article contained segments covering – Definitions, Identification Methods, Precautions, and Actions during the Incident. Based on metrics extracted from the website, the articles were viewed by 80% of the total 3200 website views.

2. Cybersecurity Online Assessment Test for MSMEs

The Cybersecurity Assessment test was developed to test the KAP of the target groups regarding common cybersecurity threats and basic digital hygiene practices to gauge the participants' KAP at the start of the campaign and to measure the shift in KAP of those participants at the end. The Assessment test consisted of 9 questions, which followed the CIA Triad to develop its questions. The CIA Triad is a common model that forms the basis for the development of security systems. They are used for finding vulnerabilities and methods for creating solutions. To gauge which parts of the CIA Triad the MSME participants are following in the business cybersecurity context, the assessment test consisted of 3 questions each on "Confidentiality," "Integrity," and "Availability."

The website post-launch, with the help of the social media campaign, saw over 400 individuals take the assessment to completion in only a month. The participants, on average, scored 5. Here, 90% of the participants scored below 7, 60% scored below 5, and an alarming 27% of the participants scored 0 out of 9 on the test. The results here further support the initial baseline assessment that revealed a major gap among MSME Cohorts regarding cybersecurity-related knowledge.

During the quarter, several early-stage collaborations were also executed with future partners like SME Foundation and media companies to reach the Laggard cohort in the higher age range of 40 – 60.

During the second quarter, several new resources were added to the website. The goal was to create a knowledge hub in the native language for the information to be widely accessible. The website was updated with 5 new knowledge articles covering different Cyber threats and introduced a new section called "Policy" that outlines the most important policies that MSMEs should be informed about to exercise their rights and be aware of the relevant legal terms that will allow their businesses to be safe and under the legal purview.

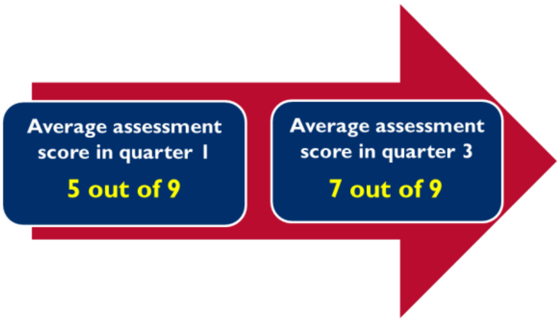

Average assessment score in quarter 1
5 out of 9
Average assessment score in quarter 3
7 out of 9

Figure 17: Average score change from quarters 1 to 3.

Due to the ongoing social media campaign activities, the website saw a surge in website visits. By the end of the second quarter, the website had over 32,000 visits and 270 additional assessment tests taken. During this quarter, a change in the average score was also observed, increasing from 5 to a much higher 7 among the test takers in the second quarter of the project.

3.1.4 The One-stop Support Desk (OSD)

Particularly after experiencing the campaign's capacity-building workshop, several MSMEs became motivated to address Cyber threats they faced but did not know how to address them before the workshop. Thus, these MSMEs started to message the campaign page requesting guidance and support as they followed the steps to counter the cyber threats they were facing. This indicated that the campaign's brand image has become a trustworthy platform that addresses cybersecurity and has built trust among its followers and beneficiaries.

> *"My page has been hacked, and I will lose my online business if don't get it back. Can you help me?"*
> **- Cyber threat victim inquiring via OSD**

> *"I lost BDT 35,000 to a supplier from whom I ordered garments in bulk. I cannot contact them, and I am worried. What can I do? Please Help!"*
> **- Cyber threat victim inquiring via OSD**

With the help of the Cybersecurity Experts part of the team and collaboration with Backdoor Pvt Ltd, which is a Cybersecurity Service provider led by one of the project experts, the campaign launched a support center named OSD to address the cybersecurity-related queries in real-time and support victims of cyber-attacks by helping them recover lost digital profiles, assets and support them in seeking help from Law enforcement.

OSD Scope of Operations:
The pilot stage of the OSD is using the campaign's Facebook page and website as the primary platform for receiving reports from MSMEs.

The support center was led by the team's cybersecurity expert—Mr. Tanvir Hassan Zoha, Assistant Professor at the Computer Science and Engineering (CSE) Department at the Bangladesh University of Business and Technology (BUBT)—and a team of three cybersecurity professionals from Backdoor Private Ltd.

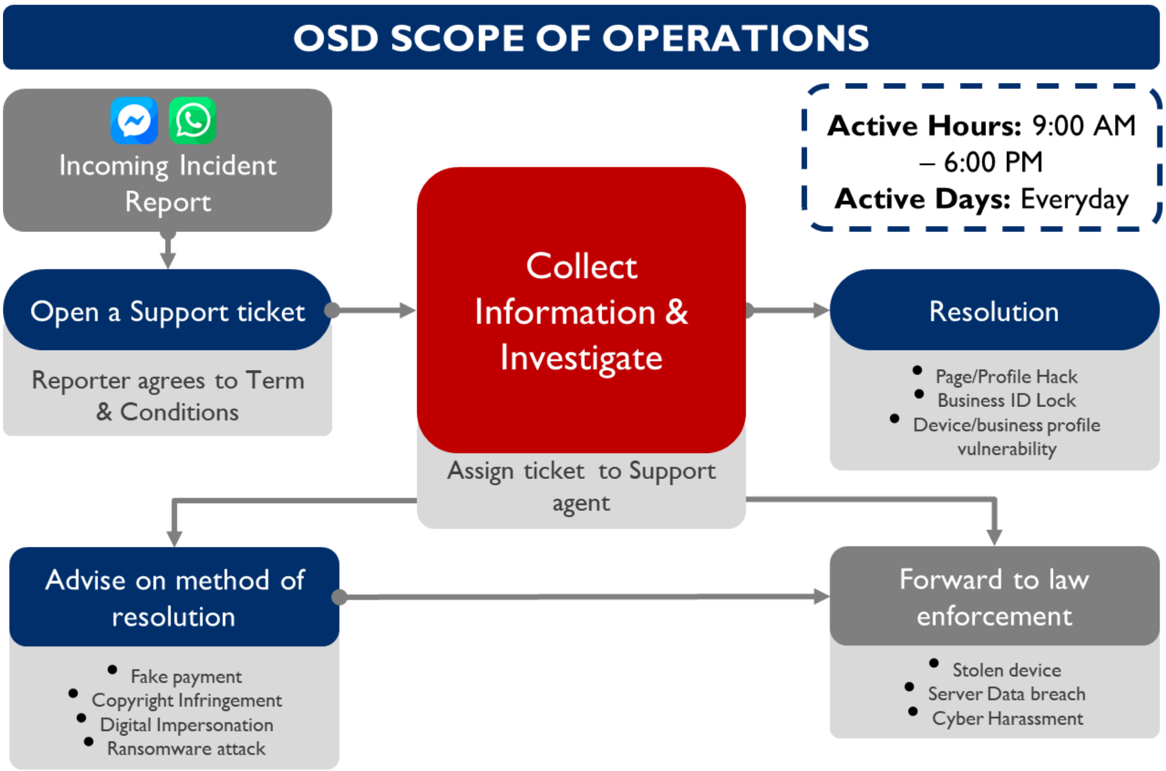


Figure 18: OSD process overview

Per the pilot's scope, the support center's operating hours are limited to regular working hours. The support process starts with submitting an incident report to the OSD's Facebook[10] Messenger or WhatsApp[11] chat. After receiving a report, the chatbot in Messenger will require the reporter to acknowledge a T&C document. After the acknowledgment, the chatbot assigns the ticket to one of the 3 representatives to respond. After receiving the support request, the representative will collect further information regarding the incident and assess which category the incident falls under. Resolutions are incidents where the support rep can provide solutions on their own. If the incident requires advising the rep of the operations lead, the rep will advise the victim on potential solutions and to-dos. Finally, if the incident is severe and requires the involvement of Law Enforcement, then they will be asked for the report to law enforcement. In this case, the support rep will assist the victim in collecting necessary information and evidence and help them write up the GD for the incident with the victim's explicit approval.

Depending on complexity, resolutions can take 2 to 7 days to resolve. There is a large spectrum of cyber threats, so the solution time varies for each.

During the second quarter, the campaign received over 190 queries. Among the 12 were incident reports from MSMEs and the general public. A total of 9 out of the 12 cases were resolved during quarter 2, and 1 case was canceled as the victim stopped responding. The majority of the cases consisted of page hacking incidents. In addition, several financial scams and lost device incident reports were among the 12 cases.

[10] (Bebshay Digital Shurokkha, n.d.)
[11] Bebshay Digital Shurokkha Incident Support Center Contact: +880 175 5555560

3.2 Offline Campaign Achievements

The campaign plans involved early-stage collaborations during quarter 1 and independent mobile activations in MSME events.

SME Foundation Collaboration:

The campaign collaborated with the SME Foundation on one of their MSME workshops on connecting MSMEs with IT companies. The session was led and organized by the SME Foundation, with over 50 MSMEs present. During the workshop, the campaign was given an exclusive segment to talk about the campaign, take a short session on MSME Cybersecurity, and finally distribute Campaign leaflets that connected the MSMEs in the session to the campaign page and website through a QR code. Several MSMEs also took the assessment test and shared their thoughts during the session.

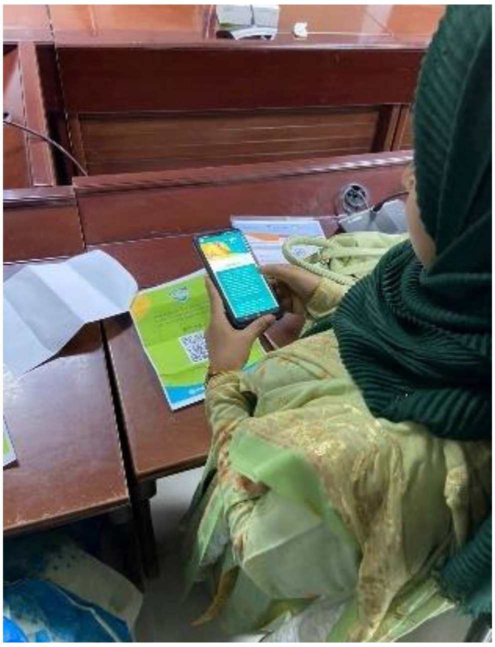


Figure 19: QR code scanning.

MSME Fair and Event Collaborations:

The campaign also reached out to open MSME Fairs and MSME Meetup events to promote the campaign's messages and encourage MSMEs to engage with the content. The event activation in quarter 1 was a collaboration with a bKash-arranged meetup on Online Community Management. The campaign team got to participate in the session and promote the campaign to 150 MSMEs present.

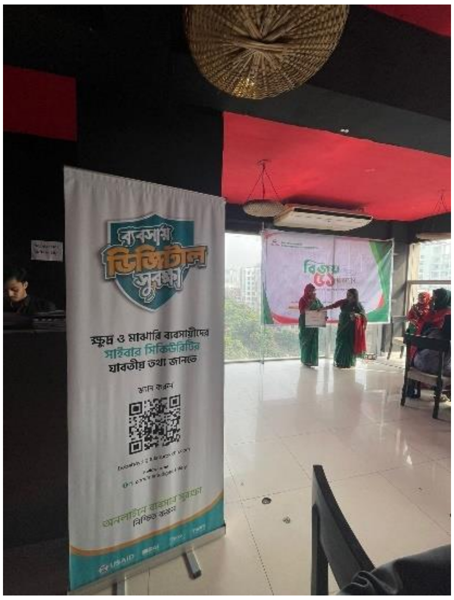
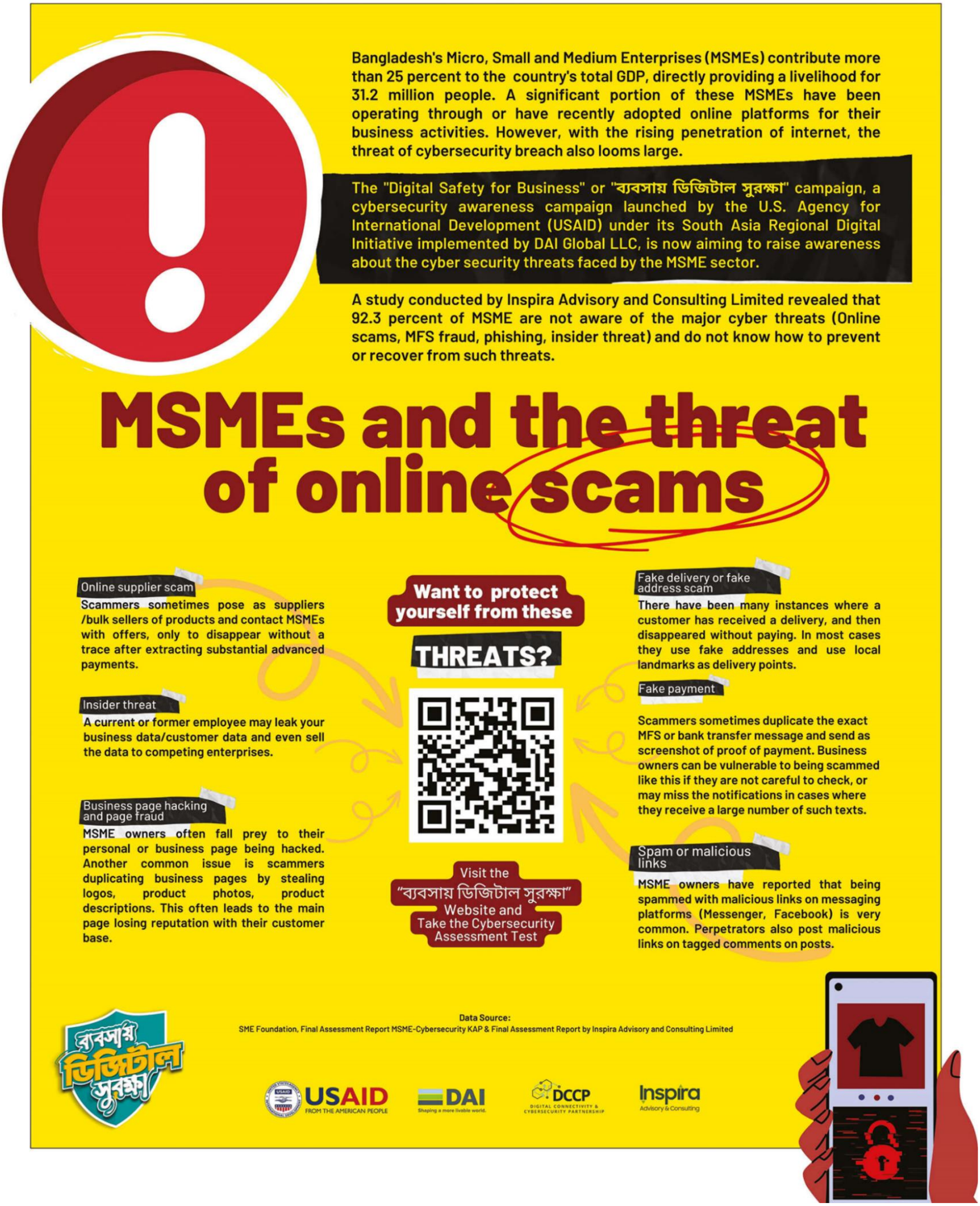


Figure 20: QR code poster

Featured in the weekly special "TOGGLE" by THE DAILY STAR:

To maximize media outreach to the Ardent Audience, including Small to medium-sized businesses, the campaign worked with The Daily Star Newspaper to share a front-page feature on their weekly special Toggle, a weekly paper focusing on technology and innovation.



Bangladesh's Micro, Small and Medium Enterprises (MSMEs) contribute more than 25 percent to the country's total GDP, directly providing a livelihood for 31.2 million people. A significant portion of these MSMEs have been operating through or have recently adopted online platforms for their business activities. However, with the rising penetration of internet, the threat of cybersecurity breach also looms large.

The "Digital Safety for Business" or "ব্যবসায় ডিজিটাল সুরক্ষা" campaign, a cybersecurity awareness campaign launched by the U.S. Agency for International Development (USAID) under its South Asia Regional Digital Initiative implemented by DAI Global LLC, is now aiming to raise awareness about the cyber security threats faced by the MSME sector.

A study conducted by Inspira Advisory and Consulting Limited revealed that 92.3 percent of MSME are not aware of the major cyber threats (Online scams, MFS fraud, phishing, insider threat) and do not know how to prevent or recover from such threats.

MSMEs and the threat of online scams

Online supplier scam

Scammers sometimes pose as suppliers /bulk sellers of products and contact MSMEs with offers, only to disappear without a trace after extracting substantial advanced payments.

Insider threat

A current or former employee may leak your business data/customer data and even sell the data to competing enterprises.

Business page hacking and page fraud

MSME owners often fall prey to their personal or business page being hacked. Another common issue is scammers duplicating business pages by stealing logos, product photos, product descriptions. This often leads to the main page losing reputation with their customer base.

Want to protect yourself from these THREATS?

Visit the "ব্যবসায় ডিজিটাল সুরক্ষা" Website and Take the Cybersecurity Assessment Test

Fake delivery or fake address scam

There have been many instances where a customer has received a delivery, and then disappeared without paying. In most cases they use fake addresses and use local landmarks as delivery points.

Fake payment

Scammers sometimes duplicate the exact MFS or bank transfer message and send as screenshot of proof of payment. Business owners can be vulnerable to being scammed like this if they are not careful to check, or may miss the notifications in cases where they receive a large number of such texts.

Spam or malicious links

MSME owners have reported that being spammed with malicious links on messaging platforms (Messenger, Facebook) is very common. Perpetrators also post malicious links on tagged comments on posts.

Data Source:
SME Foundation, Final Assessment Report MSME-Cybersecurity KAP & Final Assessment Report by Inspira Advisory and Consulting Limited

Figure 21: Toggle front page

The second quarter launched the primary activity of the campaign, the MSME Cybersecurity Workshops, along with several event collaborations owing to collaboration with stakeholders present in the Campaign Launch who are interested in pursuing a partnership with the campaign. These activities are aimed at the 7 target districts of the project. The offline activities were supported by stakeholders in the MSME Sector who shared the campaign's goals and volunteered to support the campaign in any way possible. The offline activities, as stated prior was done under two categories –

1. **Cybersecurity Capacity Building Workshops:**
   One of the campaign's key objectives was to arrange capacity-building workshops for 400 MSMEs across 7 target districts. The plan to achieve this objective was launched in the second quarter. The workshop covered the following in its curriculum.

Workshop Brief: The training workshops were being arranged with MSME owners to equip them with knowledge and hands-on training on identifying and combating cybersecurity threats, becoming more secure, and keeping their businesses safe and secure. At least 400 MSMEs were planned to be capacity-built across 7 country districts: Dhaka, Chattogram, Jashore, Bogura, Cox's Bazar, Narayanganj, and Gazipur. The workshops will be a half-day session with 30-60 MSME owners.

Workshop Overview	
Workshop Title	**Cybersecurity Training Workshop for MSME Owners**
	Training Curriculum
	Pre-assessment Test
1. Overview of Cybersecurity	a. Introduction to digital literacy and cybersecurity b. Existing knowledge, attitude, and practice of cybersecurity by MSMEs c. Importance of cybersecurity for MSMEs
2. Laws and punishments related to cybercrime	a. Digital Security Act, 2018 b. Pornography Control Act, 2012 c. Money Laundering Prevention Act, 2012 d. Anti-Terrorism Act, 2009
3. Common types of threats	a. Phishing b. Ransomware c. Malware d. Insider threat e. Fake news f. Threats in mobile: Spam messages, using malicious applications, providing excessive permissions, Application send boxing vulnerability, Operating system breach/jailbreak g. Other threats: Page hacking, Fake delivery address, Online supplier scam, Fake payment
4. Best practices to safeguard information	a. Keeping software updated b. Use of antivirus c. Setting a strong password d. Applying two-factor authentication e. Authorized login f. How to retrieve a hacked page

5. Countermeasures against cybercrime	a. Step-by-step process of reporting any cybercrime b. Response Mechanism c. Investigation process
Post-assessment Test	
Workshop Feedback Form	
Learning Materials	
● Cybersecurity Best Practices Booklet ● Cybercrime-related Laws and Punishment Handout	
Participation Benefits	
● Official certification ● Food and refreshments	

Table 3: Workshop overview

Figure 22: Workshop activities snapshot

The workshop followed a 5-component curriculum covering cybersecurity, relevant legal clauses for MSME Cybersecurity, an Introduction to cyber threats, Safeguarding methods, and countermeasures. The campaign developed a cybersecurity booklet that is a guidebook containing the most used and critical cybersecurity best practices and information on the most common cyber threats. In addition, the booklet contained key contact information for different cybersecurity support from Law Enforcement and Government Agencies. The participants who completed the workshop are awarded a completion certificate supported by USAID, DAI, DCCP, and Inspira ACL. The workshop also considers the level of immediate change in the participants' KAP to gauge the workshop's effectiveness. Thus, a pre-and post-assessment test is taken using a modified version of the Website Self-assessment test based on the CIA Triad. Finally, a feedback form is also distributed among the MSMEs to understand their perception of the workshop and their further requirements regarding cybersecurity.

During quarter 2, the campaign executed a total of 5 workshops in total. The workshops were primarily held in two districts, Dhaka and Chattogram. The execution of the workshop was supported by key stakeholders in the MSMEs sector, namely the SME Foundation and the Chittagong Women Chamber of Commerce and Industries (CWCCI). Both organizations supported the campaign team, arranging the venue and relevant workshop participants. A detailed breakdown of all 5 workshops is shared below –

Workshop No	District	Place	Collaborating Org.	Male	Female	Total Participants
1	Dhaka	SME Foundation Conference Hall, Dhaka	SME Foundation	3	37	40
2	Dhaka	SME Foundation Conference Hall, Dhaka	SME Foundation	27	0	27
3	Chattogram	CWCCI Conference Hall, Chattogram	CWCCI	6	45	51
4	Chattogram	CWCCI Conference Hall, Chattogram	CWCCI	5	39	44
5	Chattogram	CWCCI Conference Hall, Chattogram	CWCCI	5	41	46
6	Cox's Bazar	Cox's Bazar Zilla Parishad, Cox's Bazar	Cox's Bazar Youth Entrepreneur's Club (CYEC)	7	15	22
7	Narayanganj	Ali Ahmed Chunka City Library and Auditorium, Narayanganj	WE	2	63	65
8	Faridpur	Bel Piatoo	WE	3	43	46
9	Khulna	District Shilpakala Academy, Khulna	WE	16	110	126
10	Jashore	Hotel City Plaza International	WE	22	72	94
11	Dhaka	Shinepukur Suites	e-CAB	21	5	26
12	Bogura	Hotel La Villa	SME Foundation	46	13	59
Total Participants				**163**	**483**	**646**

Table 4: Workshop details overview

The five workshops conducted in Quarter 2 of the campaign garnered 50 percent of the targeted workshop participants, with 208 participants in attendance. The pre-assessment and post-assessment tests also revealed interesting results: an average score from all five workshops came to 4 out of 9 in the pre-workshop assessment, and the average score in the post-workshop assessment came to 8 out of 9. This indicated that the workshop curriculum was indeed effective in its transfer of knowledge to the participants. Further details regarding the findings can be found in the report's Campaign Findings and Learnings section.

2. MSME Fair/Event Mobile Activations:

Bangladesh currently boasts approximately 7.9 million MSMEs and is growing. This exponential number was sustainable through initiatives taken by key government agencies, technologies, marketplaces, associations, and small & large communities, and the private sector. Some of these initiatives involve arranging meetups, summits, and fairs. In quarter 2, the campaign connected with the organizers of such initiatives to participate in these events by distributing leaflets, disseminating information about the campaign to participating MSMEs, and holding short seminars regarding cybersecurity to garner interest among the key cohorts. As such, following up on collaboration with some of the key stakeholders in participating in such events, in quarter 2 of the campaign, the project team collaborated with more stakeholders to conduct more target-driven event activations. Overview of the two events the campaign activation was done are as follows –

Event Name	Type of Event	Event Size	Response Rate	Activities
Chattogram IT Fair 2023	IT Fair	Stalls: 30+	50+ MSMEs and visitors responded	- Introducing the campaign - Campaign website visited through QR code scanning - Assessment test taking through QR code scanning
Chattogram SME Trade Fair 2023	MSME Fair	Stalls: 300+	Around 200 MSMEs and visitors responded	- Introducing the campaign - Leaflet Distribution - Voxpop - Campaign website visited through QR code scanning - Assessment test taking through QR code scanning

Table 5: Event overview

In the Chattogram IT Fair, the campaign team's primary objective was to understand Cybersecurity gaps among IT service providers as these service providers will often handle a large amount of data that may be sensitive as well. The activities involved quizzing the IT-based MSMEs at the fair on certain Cybersecurity best practices. However, we found even though these organizations deal with cyberspace regularly, they do not maintain many of the best practices that would be needed to protect the data they are processing and collecting. There was a lack of awareness among MSMEs in maintaining different passwords for different accounts, measures to ensure they are protected from Insider threats, and even gaps in hygiene. This was done by having them participate in the assessment test on the campaign website, with 90% of the respondents scoring around 4 to 6 out of 9.

> *"I fell for a bKash scam once. A person called me and told me that he accidently sent BDT 20,000 to me on bKash and asked me to check my messages to confirm. I saw there was a message from what I thought bKash that BDT 20,000 had been deposited. So, I immediately sent over the amount to the number he called from. However, when I went to check my balance later in the day, I realized I never received a BDT 20,000 deposit to my bKash. It was a traumatic experience for me."*
>
> **- Fair Participant**
> **A female entrepreneur from Chattogram**

In the Chattogram SME Trade Fair 2023, a much more diverse pool of MSMEs was present. As this is a large yearly event organized by the SME Foundation, we leveraged the connection with the SME Foundation to conduct impromptu interviews with the attendees to gauge their knowledge (vox pop sessions) on cybersecurity and to create awareness among the visitors and MSMEs present in the stalls. All other activities were also conducted along with the Vox Pop. Most MSMEs also showed a general gap in their understanding of the Internet and the risks of operating their businesses online. And shared their own experiences facing Cyber threats. The key gap here was their know-how of countermeasures.

The third quarter of the offline activation program consisted of MoU signing with WE, e-CAB, and BdOSN. The signing of the MoU was ceremonially done in the Inspira ACL office in the presence of the partner representatives. There were 3 interactive theater performances, namely "Gambhira," which were arranged to showcase cyber threats and countermeasures to tackle them.

Interactive Theatrical Performance (Gambhira):
The Gambhira was arranged in 3 districts, namely, Jashore, Bogura, and Khulna, by a vendor called Sundarban Theatre, and it was mainly targeted at the laggard group of people in rural areas who have low cyber knowledge and comprehension of it. The theatre performances were conducted with music and actors who attractively acted out a certain cyber threat incident story and called the audience on stage to question their knowledge and how they dealt with cyber threats if they faced any. We also gave the audience who gave the most appropriate answers the custom cybersecurity ludo board as a gift. We reached about 500 participants through these interactive theatrical performances.

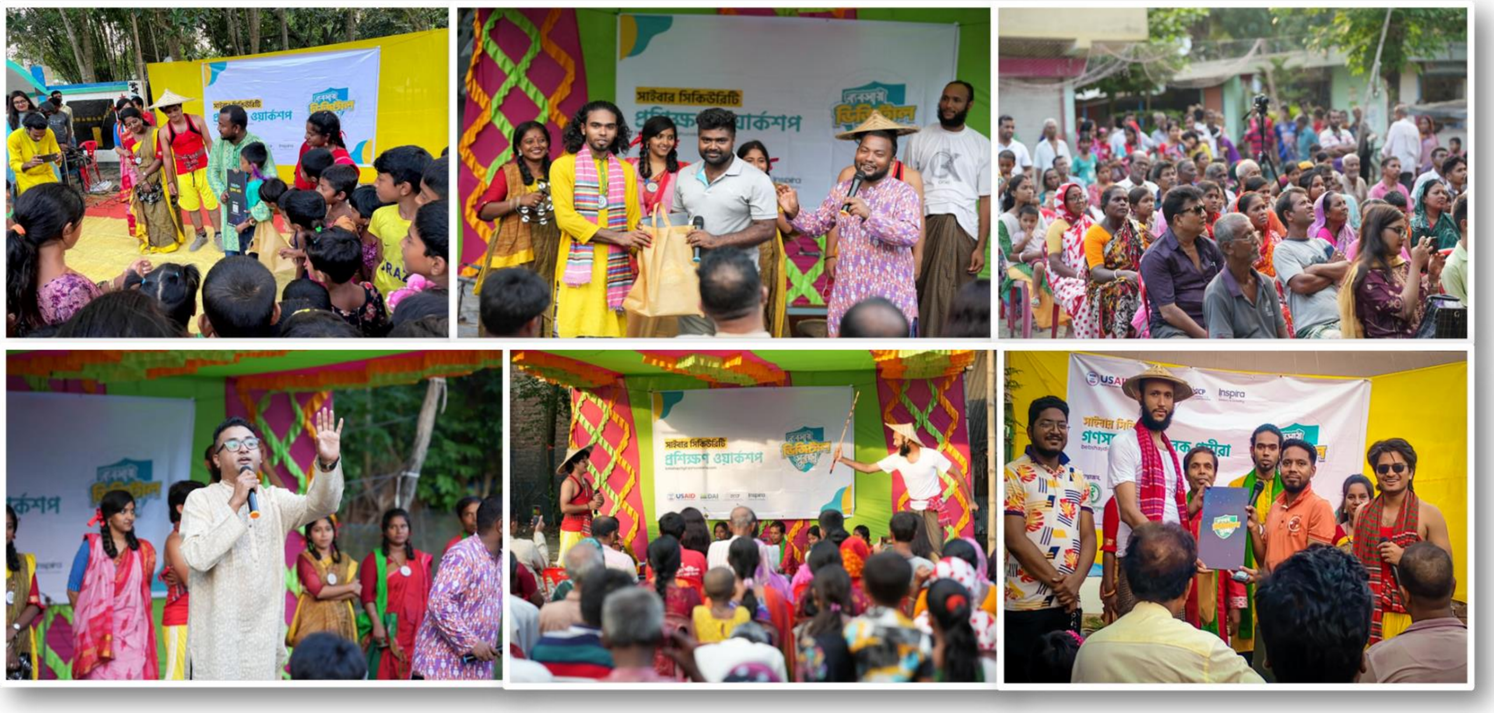


Figure 23: Gambhira snapshot

3.3 Partnership Achievements

Figure 24: Partnership Meeting

Partnerships were an instrumental part of this campaign's design. The MSME sector is affected, supported, and facilitated by several Government agencies, Associations, Communities, Financial Institutions, and e-Commerce Platforms. During the first quarter, the campaign focused on establishing relations with the key stakeholders of the MSME sector in Bangladesh and initiating collaborations as a first step to establishing a partnership, inviting representatives from these entities to attend.

To that end, the campaign organized a live Campaign Launch Event hosted by The Daily Star through their Facebook page. The main event focused on a keynote speech explaining the context and findings from the campaign's assessment report on the current scenario of cybersecurity awareness of the target groups of the project as well as factors such as their understanding of cybersecurity terms, level of vulnerability to Cyber Attacks and awareness of measures that can secure online information and data.

> *"I would like to invite the Campaign team to collaborate with SME Foundation and bring this important messaging using our extensive network, especially during our upcoming SME FAIR 2022."*
>
> **Dr. Md. Mafizur Rahman**
> **Managing Director of SME Foundation**

Campaign Inauguration and Launch Event: The Launch event was held on October 26th, 2022, at The Daily Star Headquarters in collaboration with them to cover the event live. The event was joined by respected government directorates, private sector leaders, law enforcement deputies, business associations, and community leaders, all direct stakeholders of Bangladesh's growing MSME sector. The launch event was joined by Project Management Specialist (Private Sector Development), The Office of Economic Growth, USAID Bangladesh Ms. Aklima Haque, SME Foundation Managing Director Dr. Md. Mafizur Rahman, a2i (Aspire to Innovate) Project Director and Joint Secretary Dewan Muhammad Humayun Kabir and Additional Deputy Police Commissioner of the Cyber Crime Investigation Division of the Counter Terrorism and Transnational Crime (CTTC) unit at the Dhaka Metropolitan Police, Md. Najmul Islam at the inauguration ceremony. The Director of Direct Fresh Ltd., Mr. Zeeshan Kingshuk Haq, hosted the ceremony.

The event engaged parties from all three key stakeholder groups in an enlightening discussion addressing some of the core issues the MSMEs have faced regarding cybersecurity and their digital safety. The discussion also covered the systemic barriers currently demotivating MSMEs from taking action against their Cyber Perpetrators and what can be done to resolve the issue.

The discussion revealed the current challenges that MSMEs face when reaching out to law enforcement regarding these issues, and it was noted that the further expansion of the Bangladesh Cyber Crime Investigation Division of CTTC and capacity building of Law enforcement personnel would be crucial to a more swift and effective resolution to Cyber Attacks. The panel unanimously agreed that the initiative is an important one and urged that more such initiatives be taken to address the looming cyber threats that have been slowly growing in intensity and complexity.

The session also explored the impact of cyber threats beyond vulnerable MSMEs. The Project Director of a2i, Humayun Kabir, highlighted the current threat to Bangladesh youth and adolescents regularly exposed to the internet without parental supervision or appropriate device security.

> *"Cybersecurity awareness needs to be incorporated in education curriculum starting from primary level so it can be embedded into people at a younger age."*
> **Dewan Mohammad Humayun Kabir**
> **Project Director (Joint Secretary) of a2i**

In quarter 2 of the campaign, to execute all planned activities, the campaign team utilized its network built through the campaign launch event to execute the partnership opportunity mapping and subsequent outreach efforts.

One of the most crucial achievements in this quarter was a joint discussion session with all potential partners and USAID to consider the sustainability of the campaign activities and opportunities for public-private partnership to achieve the broader goal of the parent project of the campaign, the South Asia Regional Digital Initiative (SARDI). The session aligned the Government and private sector representatives on the project's objectives and their role in achieving the project's goal to strengthen the nation's Cybersecurity and bring meaningful change to the policies related to Cybersecurity and MSMEs.

Among the above-listed partners, the prioritization of the partners was based on their compatibility with the different opportunities.

Partnerships or collaborations were established with the following organizations to achieve the stated partnership activities in quarter 2 –

SL	Organization	Discussed Partnership Activities
1	SME Foundation	a. Workshop Collaboration: 2 workshops in Dhaka b. Social Media Collaboration: 2 collaboration posts were shared to increase campaign visibility among SME Foundation Followers
2	BdOSN	a. Social Media Collaboration: Access to the BdOSN community and the "Chakri Khujbo na Chakri Dibo" MSME community to share campaign content, promote the website, webinars, and workshops. 5 Learning and workshop promotional content shared
3	WE	b. Workshop Collaboration: 4 Workshops in Narayanganj, Faridpur, Khulna, Jessore c. Social Media Collaboration: 2 promotional posts featuring WE as a partner to the campaign, 4 Workshop posts, 4 Community forums connected to each workshop location
4	e-CAB	a. Workshop Collaboration: 1 Workshop in Dhaka with unconventional sectors such as e-commerce startups, Digital Marketing firms, Private Security and Cybersecurity Firms, BPOs, Hotels, etc.
5	Backdoor Private Limited	a. One-stop Support Center for Cyber Incidents: Launch of a text-based support center with

Table 6: Partners and activities

During the campaign's run, several other opportunities were discussed with the potential partners that may enrich the campaign's overall impact, and its messaging spread further among more MSMEs across Bangladesh.

Several opportunities were discussed with the potential partner to proliferate the campaign messaging to reach the most people, such as collaboration with bKash, Nagad, and Foodpanda to place campaign messaging in their app and website and send awareness-based messaging through push notifications. Beyond that, Bank Asia and BRAC Bank also discussed “training of trainers” for their SME agents so they can proliferate the campaign's messaging and incorporate a process to build the capacity of the MSMEs who are their clients to be more cyber resilient. This allows the banks to reduce risk on investment.

However, one of the most exciting opportunities was discovered through frequent interaction with the direct beneficiaries themselves. During the middle of Quarter 2, several messages were received from MSMEs and individuals reporting incidents to the Facebook page and asking whether the campaign could help. Thus, an additional collaborative component was added to the campaign: a Support Center to address Cyber Incidents with the help of experts in the field.

Part 4

RECOMMENDATIONS

4.0 Key Recommendations

To achieve project objectives, the project team came across several challenges and unexplored potential beyond the initial planning and project scope. In addition to that, as the project engaged with the key beneficiaries and stakeholders, several new opportunities were discovered that would effectively achieve the larger goal of the SARDI initiative in Bangladesh. To that end, the recommendations for the project will be showcased under two broader segments –

1. Recommendations for Similar Initiatives
2. Learnings that informed Planning of a Second Phase

5.1 Recommendations for Similar Initiatives

Based on lessons learned during the execution of the planned activities for the campaign, the project team has formulated 4 key areas of focus to maximize the effectiveness, reach, and sustainability of a similar campaign –

5.1.1 Partnerships as Amplifiers

PARTNERSHIPS AS AMPLIFIERS

Considering the target group (TG), engaging in forming partnerships and collaborations with key stakeholders can amplify reach while maximizing impact at the same time.

- **Amplification of Reach**
  Through partnerships with platforms, key industry associations, community groups connected to the TG
- **Amplification of Activations**
  Partnerships with associations and organizations responsible for arranging events for or with the TG
- **Amplification of Resources**
  Partnerships with institutes and organizations already engaged in activities similar to project activities can allow utilization of partner resources to execute activities with enhanced efficiency

Figure 25: Partnership recommendations

1. **Amplification of Activation**

The campaign's success was largely owed to the partners and collaborators who supported the organization of the campaign activities. The campaign was able to leverage the partnerships to ***amplify project activations***. For example,

a. *We partnered with SME Foundation, CWCCI, e-CAB, and Women and E-commerce Trust to facilitate successful workshops for MSMEs' awareness and behavioral change regarding cybersecurity best practices.*

b. *We collaborated with bKash and some smaller MSME communities to arrange livestream Q&A sessions and participate in MSME Fairs, meet n Greets, and Interactive Theater Performances.*

2. **Amplification of Reach**

   The campaign's core target group of MSMEs across 8 districts had varying ranges of reachability and engagement potential due to varied factors such as access to the internet, understanding of cybersecurity issues, level of business-related engagement in digital platforms, and geographic location. As such, a reliable method of reaching MSMEs that are particularly difficult to approach through digital marketing is to connect with local communities, associations, and trade organizations who can act as liaisons to convey campaign messaging and activities and advise on the most effective awareness initiatives for specific locals for more informed activations. For example –

   a. Collaborating with community groups and online e-commerce platforms prominent in target districts to share campaign messaging through co-branded content, live streams, webinars, and joint events.
   b. Partnering with local associations and trade organizations responsible for arranging fairs, events, and MSME development initiatives to arrange joint awareness activations to maximize relevant participation and improve reach.

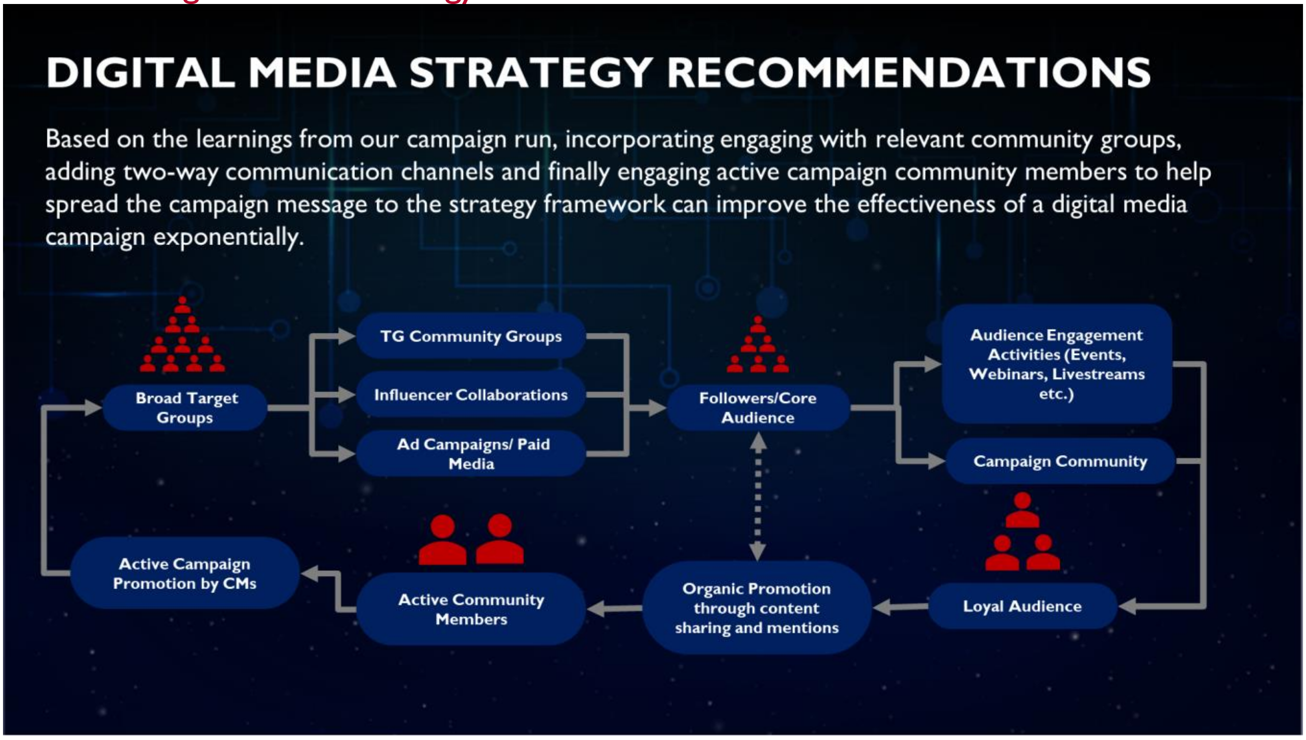
3. **Amplification of Resources**

   Any awareness activation initiatives will require resources tied to different activities that may be challenging to acquire in certain locations. This resource gap is typically observed in the pre-urban and rural regions. For arranging initiatives in regions less accessible for information on arranging event venues, equipment, and logistics support.

   Partnering with organizations with available local venues, training centers, and local teams can make executing a local activation a much simpler process. For example,

   a. During the collaboration with CWCCI, the partner representatives assisted the organizing team in arranging logistics, contacted workshop participants, and coordinated with the core team to facilitate the event, which made the overall execution a further streamlined process.

5.1.2 Digital Media Strategy Recommendations



DIGITAL MEDIA STRATEGY RECOMMENDATIONS

Based on the learnings from our campaign run, incorporating engaging with relevant community groups, adding two-way communication channels and finally engaging active campaign community members to help spread the campaign message to the strategy framework can improve the effectiveness of a digital media campaign exponentially.

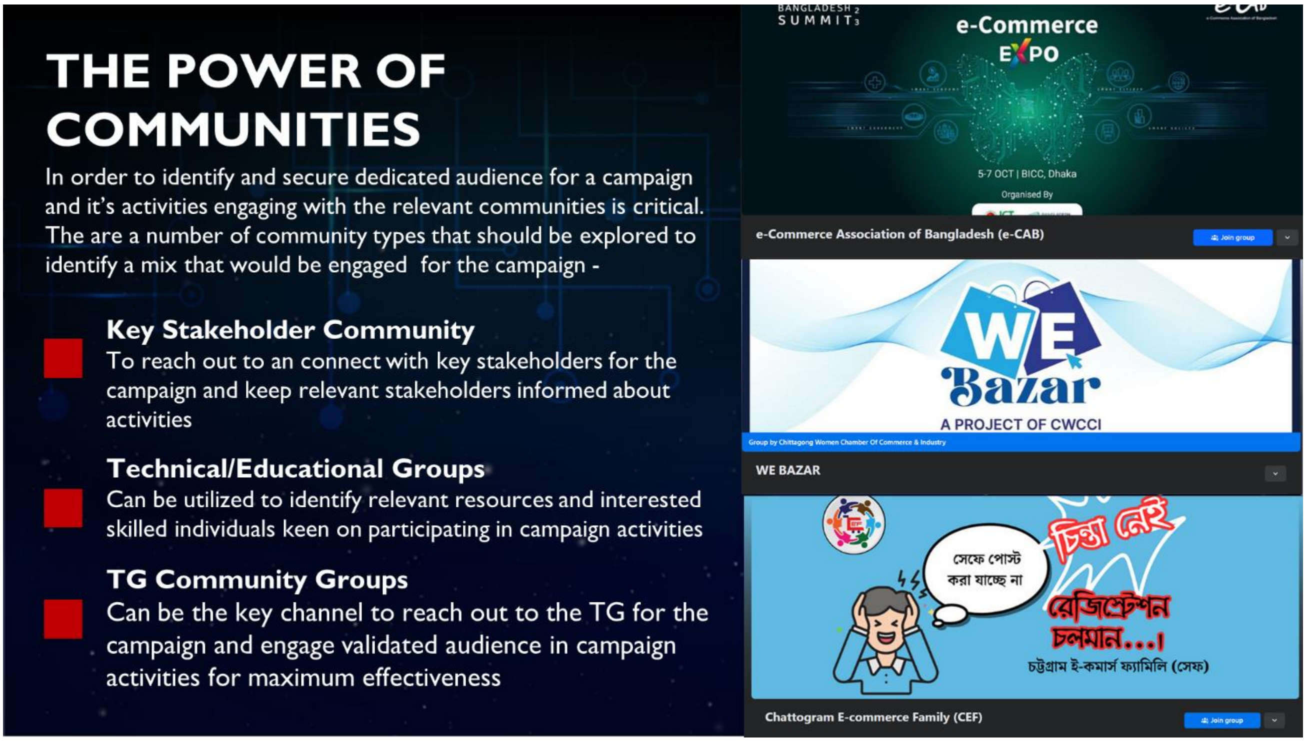
Broad Target Groups
TG Community Groups
Influencer Collaborations
Ad Campaigns/ Paid Media
Followers/Core Audience
Audience Engagement Activities (Events, Webinars, Livestreams etc.)
Campaign Community
Loyal Audience
Organic Promotion through content sharing and mentions
Active Community Members
Active Campaign Promotion by CMs

Figure 26: Digital Media Strategy Recommendations

Considering the subject matter and target groups of an awareness campaign, digital media campaigns are often the most effective method for reaching a large pool of target audiences and engaging the target groups to proceed through the campaign's marketing funnel. The strategy framework showcased here has considered incorporating multiple channels throughout each section of the funnel to take the intended target groups through some channels of engagement to filter the audience from followers to loyal Audience to community members who would be actively engaged in expanding the reach of the campaign messages to create Knowledge, Attitude and Practice level changes.

Within the strategy, we have added several components to improve its effectiveness to achieve the campaign goal of creating behavioral change with sustainability components for long-term impact among the target group. The key additions are as follows –

1. Community Group Engagement



THE POWER OF COMMUNITIES

In order to identify and secure dedicated audience for a campaign and it's activities engaging with the relevant communities is critical. The are a number of community types that should be explored to identify a mix that would be engaged for the campaign -

Key Stakeholder Community
To reach out to an connect with key stakeholders for the campaign and keep relevant stakeholders informed about activities

Technical/Educational Groups
Can be utilized to identify relevant resources and interested skilled individuals keen on participating in campaign activities

TG Community Groups
Can be the key channel to reach out to the TG for the campaign and engage validated audience in campaign activities for maximum effectiveness

Figure 27: Community Engagement Recommendations

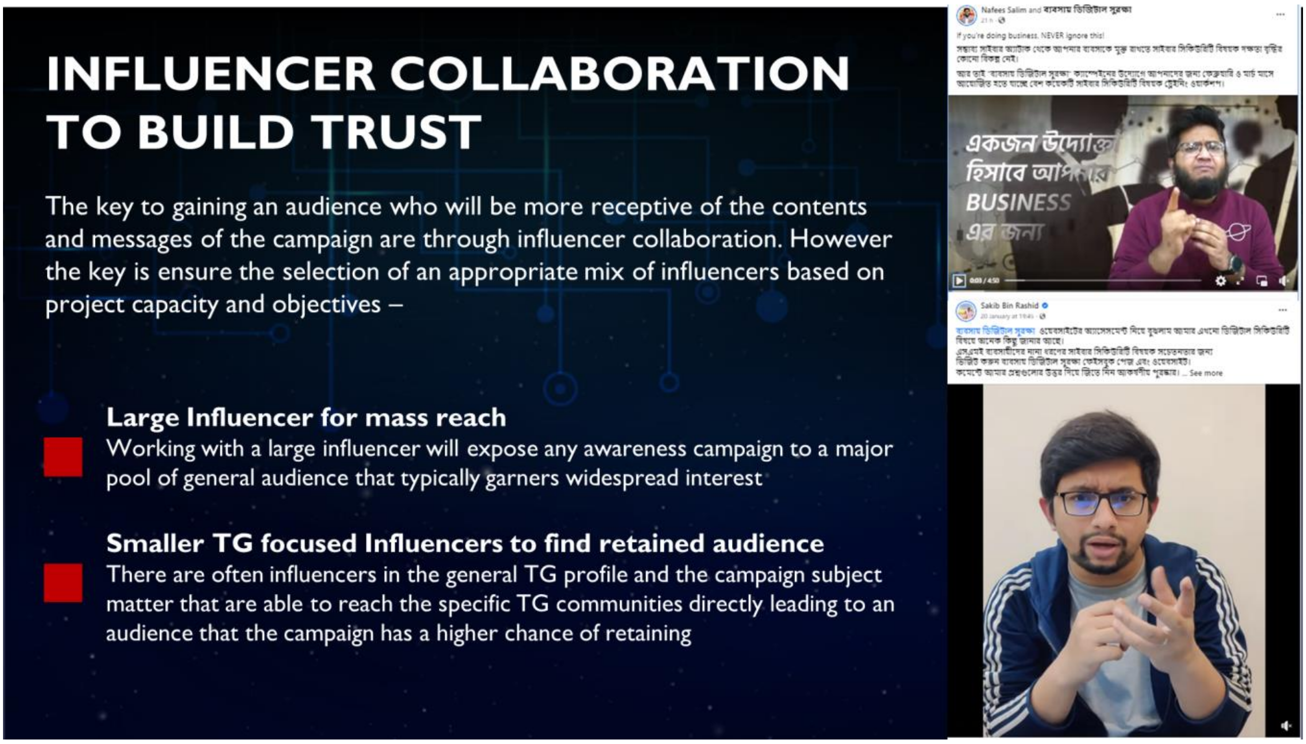
To boost the initial reach when launching a digital media campaign, garnering organic audience through engaging relevant community groups identified through researching the current market landscape and key influential stakeholders.

Based on the need gap assessment conducted at the start of the project on the Bangladesh MSME landscape, there are some major communities, as well as a large number of districts, focused on smaller communities of active MSMEs who have been running these groups to support each other and develop their businesses. Beyond these groups, groups with active members who are key stakeholders and communities with industry-related practitioners who discuss the campaign's key subject are ideal platforms for engaging awareness and behavioral change campaigns. The following activities are recommended for effective community engagement –

- Learning and awareness content promotions in collaboration with community admins
- Holding live streams and online learning sessions with community members to inform and engage them in awareness-creation activities
- Engaging community groups to participate in engaging quizzes and online activations to generate interest

- Collaborating with community groups to arrange in-person events and activities to improve rapport and build better relations

2. **Collaborating with interesting content creators**



INFLUENCER COLLABORATION TO BUILD TRUST

The key to gaining an audience who will be more receptive of the contents and messages of the campaign are through influencer collaboration. However the key is ensure the selection of an appropriate mix of influencers based on project capacity and objectives –

Large Influencer for mass reach
Working with a large influencer will expose any awareness campaign to a major pool of general audience that typically garners widespread interest

Smaller TG focused Influencers to find retained audience
There are often influencers in the general TG profile and the campaign subject matter that are able to reach the specific TG communities directly leading to an audience that the campaign has a higher chance of retaining

Nafees Salim and ব্যবসায় ডিজিটাল সুরক্ষা
21 h ·

If you're doing business, NEVER ignore this!

সম্ভাব্য সাইবার অ্যাটাক থেকে আপনার ব্যবসাকে মুক্ত রাখতে সাইবার সিকিউরিটি বিষয়ক দক্ষতা বৃদ্ধির কোনো বিকল্প নেই।

আর তাই 'ব্যবসায় ডিজিটাল সুরক্ষা' ক্যাম্পেইনের উদ্যোগে আপনাদের জন্য ফেব্রুয়ারি ও মার্চ মাসে আয়োজিত হতে যাচ্ছে বেশ কয়েকটি সাইবার সিকিউরিটি বিষয়ক ট্রেইনিং ওয়ার্কশপ।

Sakib Bin Rashid
20 January at 19:45 ·

ব্যবসায় ডিজিটাল সুরক্ষা ওয়েবসাইটের অ্যাসেসমেন্ট দিয়ে বুঝলাম আমার এখনো ডিজিটাল সিকিউরিটি বিষয়ে অনেক কিছু জানার আছে।
এসএমই ব্যবসায়ীদের নানা ধরণের সাইবার সিকিউরিটি বিষয়ক সচেতনতার জন্য
ভিজিট করুন ব্যবসায় ডিজিটাল সুরক্ষা ফেইসবুক পেজ এবং ওয়েবসাইট।
কমেন্টে আমার প্রশ্নগুলোর উত্তর দিয়ে জিতে নিন আকর্ষণীয় পুরস্কার। ... See more

Figure 28: Influencer Collaboration Recommendations

In the current digital landscape, online influencers, both large and small, are the source of trust for their respective audiences and can greatly sway them towards activities and behavioral habits. Influencers can range from niche to broad audiences; as such, there is a good amount of flexibility to collaborate with them based on campaign scope. Through the campaign collaboration, we have discovered some key considerations when identifying influencers to collaborate with -

1. Smaller but more audience-relevant influencers will garner a more dedicated following and a more responsive audience.
2. The scope and nature of the collaboration should be planned considering the influencers' SoP. Also, integrating the influencer into the campaign goals and objectives leads to better overall outcomes.
3. Thus, utilizing audience-relevant influencers is crucial to building a dedicated following in campaign platforms, improving the campaign's further organic reach and overall page health.

3. Converting beneficiaries into campaign spokespersons:

Onboarding beneficiaries of the campaign to then become the voice of the campaign is an effective strategy that would allow for authentic word-of-mouth marketing and non-financially incentivizing such effort and even creating opportunities for beneficiaries to become part of the campaign will be an effective way to spread the branches of communication channels for similar campaigns. For this activity, beneficiaries can be utilized in the following manner –

1. Campaign Ambassadors: Active community members engaging with the campaign can be motivated by having them directly engage in campaign efforts such as promoting campaign messages, acting as moderators in the campaign community to lead discussions, assisting in campaign activations as volunteers, and more.
2. Liaison for connecting with other relevant communities: Certain beneficiaries may also have their connections that could be capitalized on to expand organic outreach initiatives

4.2 Learnings that Informed Planning of a Second Phase

4. **Any campaign addressing MSME owners of Bangladesh should leverage a mixed-method communications strategy leveraging both offline P2P networks and social media:**

MSME entrepreneurs value peer connection for solving any business-related problems. Thus, involving peer-to-peer networks and industry associations at the cluster level should be an effective campaign strategy. However, most of the respondents from the survey and FGDs have online footprints and thus prefer online content to get knowledge on cybersecurity.

Ardent and Laggard target groups face distinctly different cyber threats and thus have different awareness needs. Their learning habits and media preferences also differ; hence, the campaign activities will have to feature different messaging and activities reflecting the specific requirements of each group.

5. **The campaign should follow a 'standard approach' so that the target group (TG) can expand its horizon of understanding regarding cybersecurity gradually:**

The campaign should be divided into three quarters, each phase serving a different purpose in orienting the TG with cybersecurity awareness. The first phase will educate the audience regarding the various types of cybersecurity threats that MSME owners are predominantly facing in Bangladesh, the next phase will educate regarding protective measures and provide reassurance that these threats can be prevented, and finally, Phase three will aim to ensure that cybersecurity habits and internet hygiene become a greater part of the collective consciousness.

6. **To resonate with the MSME target group, the messaging of the campaign has to follow a simplistic, casual, and storied approach:**

Analysis of existing awareness content reveals that statistical data and stringent *"Do's and don'ts"* messaging are ineffective in capturing the target segment's attention. Consequently, the campaign messages will be disseminated through case stories, comic strips, engaging social media posts, and short instructional videos to maintain relatability with the target group. The content will be designed with the target segment's ease of consumption.

7. **The campaign should have a common platform that provides a content repository that would contain all the learning resources prepared for MSME owners:**

To ensure that the resources are maintained beyond the campaign timeline, all the resources will be available on a dedicated website. As web searches of the website will be initially limited among the target group, the campaign's social media content will be designed to capture their attention online and redirect them to the appropriate resources.

8. **Expansion Of Scope in Cybersecurity Training:**

During phase I activation of Cybersecurity workshops, 50% of the core beneficiaries expressed the need for more in-depth training on specific cybersecurity topics most relevant to their business, chief of them being protection and legal action mechanisms in case of Business Page Hacks, Projection against spam messages, fake news identification and online scams.

The workshop partners (SME Foundation, CWCCI, Bank Asia, etc.), who are financial organizations, large communities, and associations, have expressed the need for their own MSME Development Trainers to be trained in Cybersecurity as well so they can, in turn, expand the reach of the training program.

9. **The Development Of Sustainable Mechanisms and Solutions Are Needed:**

Both partners and USAID raised concerns regarding the sustainability and lasting impact of the project. To that end, developing a running platform focused on cybersecurity was mutually agreed upon for the next action.

10. **Cyber Laws and Policies Have Room for Improvement:**

According to the CTTC DMP, a2i, and the project Cyber Law Consultant, critical gaps in the Cyber Laws of Bangladesh are no longer effective and require revision to create a space where small businesses can rely on cyber laws to operate their businesses safely.

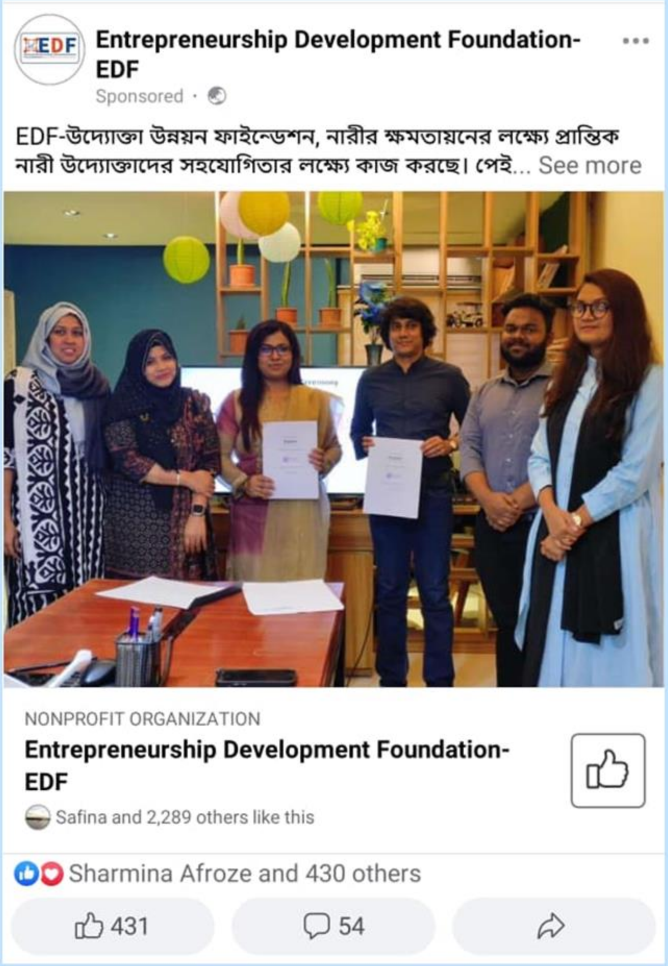
11. **Partnering With Smaller Community Organizations and Associations Can Lead to Higher Impact:**

Smaller organizations such as independent MSME social media communities have proven to be very effective partnerships in phase. While their reach is limited, they effectively reshare awareness and assist in selecting workshop participants.

12. **Ownership of Campaign Content and Caution Over Plagiarism:**

Throughout the campaign, the Inspira team faced 3 instances where the campaign's resources, images, content, or partner identities were plagiarized and used without permission from the proper authority.

The 3 instances below illustrate the various plagiarism issues that may arise.



Entrepreneurship Development Foundation-EDF

Sponsored ·

EDF-উদ্যোক্তা উন্নয়ন ফাইন্ডেশন, নারীর ক্ষমতায়নের লক্ষ্যে প্রান্তিক নারী উদ্যোক্তাদের সহযোগিতার লক্ষ্যে কাজ করছে। পেই... See more

NONPROFIT ORGANIZATION

Entrepreneurship Development Foundation-EDF

Safina and 2,289 others like this

Sharmina Afroze and 430 others

431 54

Plagiarism Case 1: Fake Partner Page

-Women & E-commerce Trust (WE), our campaign partners, reported a fake Facebook community impersonating some of their members and shared our MoU signing picture with a fake caption.

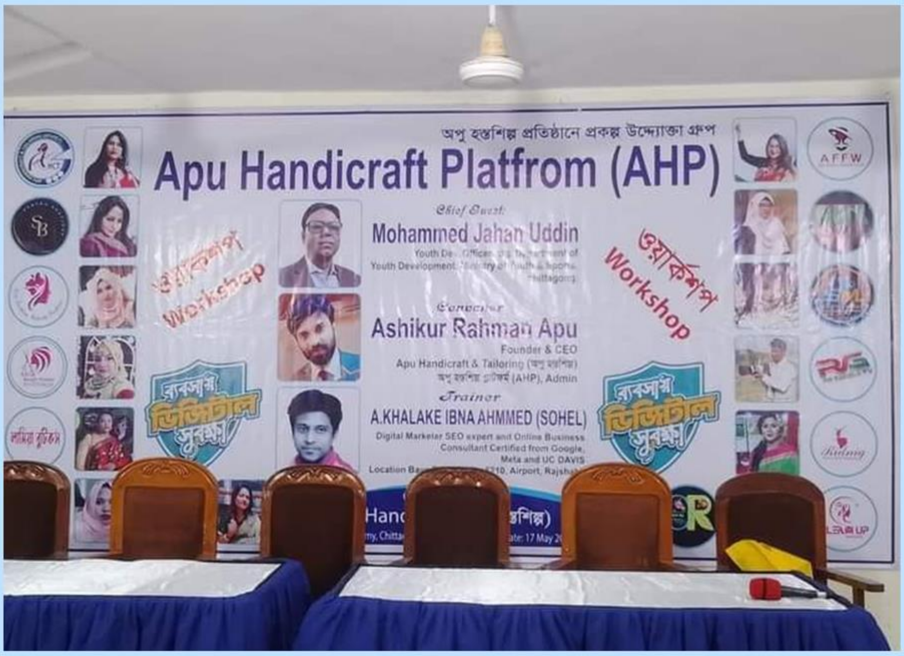
-As of May, the fake page had nearly 3k followers, most of whom were entrepreneurs.

-The campaign's cyber experts have reported the page to Meta authorities, and have traced the IP from which the page was created.

-The fake page also featured other entrepreneurship-related content, many of which were determined to be misinformation posts.

-The page was reported to Meta authorities and has since been inactive.

Figure 29: Plagiarism Case 1


অপু হস্তশিল্প প্রতিষ্ঠানে প্রকল্প উদ্যোক্তা গ্রুপ
Apu Handicraft Platfrom (AHP)
Chief Guest:
Mohammed Jahan Uddin
Convener
Ashikur Rahman Apu
Founder & CEO
Trainer
A.KHALAKE IBNA AHMMED (SOHEL)
Workshop
ওয়ার্কশপ

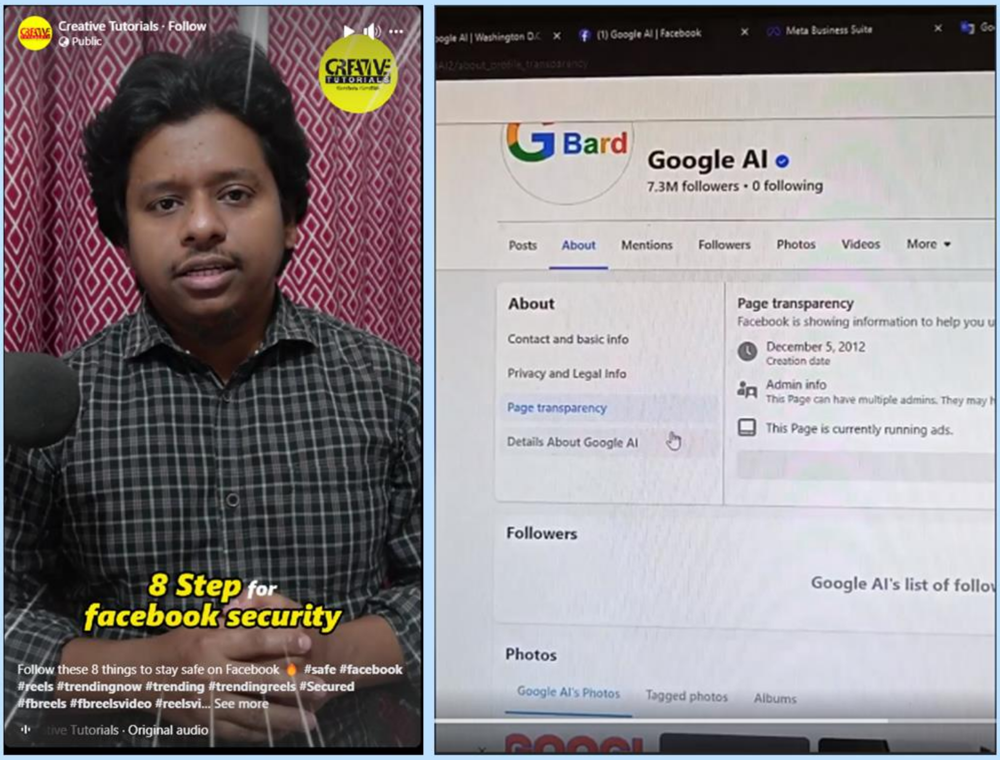
Plagiarism Case 2: Fake Workshop

Chittagong Women's Chamber of Commerce and Industries (CWCCI) reported in May that they noticed a workshop host using our campaign logos on their banner.

-The workshop was for capacity building of entrepreneurs in the handicraft sector, and CWCCI noticed the use of our logos when their chairman was invited as a guest at the event.

-The campaign team reached out to the organizer, who mentioned that he had instructed a designer to make the banner for him, who accidentally copied our campaign logo from the web.

Figure 30: Plagiarism case 2


Creative Tutorials · Follow
Public
CREATIVE TUTORIALS
8 Step for facebook security
Follow these 8 things to stay safe on Facebook #safe #facebook #reels #trendingnow #trending #trendingreels #Secured #fbreels #fbreelsvideo #reelsvi... See more
Tutorials · Original audio
Google AI | Washington D.C.
(1) Google AI | Facebook
Meta Business Suite
Bard
Google AI
7.3M followers • 0 following
Posts
About
Mentions
Followers
Photos
Videos
More
About
Contact and basic info
Privacy and Legal Info
Page transparency
Details About Google AI
Page transparency
Facebook is showing information to help you u
December 5, 2012
Creation date
Admin info
This Page can have multiple admins. They may h
This Page is currently running ads.
Followers
Google AI's list of follo
Photos
Google AI's Photos
Tagged photos
Albums

Plagiarism Case 3: Facebook content based on Workshop content

One of our workshop participants, Mr. Nasim, has started creating his own short videos taking "inspiration" from our workshop content.

Mr. Nasim's Facebook page, titled " Creative Tutorials" features videos such as short explainers on basic Facebook security, identifying fake pages, and how to avoid online scams. It was evident to the campaign team that the content was lifted right from our workshop materials.

Despite the plagiarism here, this was overall a net positive, as people witnessing his content would still be informed and more aware.

Figure 31: Plagiarism case 3

For the first two cases, the team had to take action to stop the misuse of the campaign's image and resources. On the third instant, we converted Mr. Nasim into an advocate for the campaign, and he became a "micro-influencer," helping to spread cybersecurity awareness to other MSME owners within his network.

Annex-1: Offline Activity Data

Activity Title: Campaign Launch Event
Description: MSME Cybersecurity Stakeholder discussion and inauguration of the SARDI MSME Cybersecurity Campaign (Bebshay Digital Shurokkha)
Location: The Daily Star Head Office (Conference Room)
Date: 27 October 2022
Link: https://www.thedailystar.net/business/economy/news/usaid-launches-cybersecurity-campaign-3153321

SL	Name of Speaker	Designation	Organization
1	Aklima Haque	Project Management Specialist (Private Sector Development), The Office of Economic Growth, USAID Bangladesh	USAID
2	Dr. Md.Mafizur Rakhman	Managing Director	SME Foundation
3	Dewan Mohammad Humayun Kabir	Project Director (Joint Secretary)	a2i
4	Md. Najmul Islam	Additional Deputy Police Commissioner	Cybercrime Investigation Division, CTTC, DMP
5	Zeeshan Kingshuk Huq	Chief Marketing Officer	Direct Fresh
6	Rezwanul Haque Jami	Head of e-Commerce	a2i
7	Nasima Aktar Nisha	Founder and President (WE), Joint Secretary (e-CAB)	WE & e-CAB
8	Samira Zuberi Himika	Senior Vice President	BASIS
9	Md. Saimum Reza Talukder	Senior Lecturer	School of Law BRAC University
10	Sanzida Chowdhury Swarna	Founder	Shreya Bangladesh
11	Kazi Mustafiz	President	CCAF
12	Biplob Ghosh Rahul	CEO	E-courier
13	Janefar Alam	Managing Director	CODS (Cyber Operation and Digital Solution) & Trade wave technology
14	Tanvir Hassan Zoha	Assistant Professor/cybersecurity expert	Bangladesh University of Business and Technology
15	Jamal Yusuff Zuberi	Director of Finance	Foodpanda
16	Md. Ishtiaque Masroor	Brand Manager	Shopup
17	Sajibur Rahman	Journalist	Financial Express
18	Muntasir Tahmeed Chowdhury	Managing Director	Inspira Advisory and Consultancy Limited
19	Md. Samiul Anam	AVP & Head of CMSE Business, Channel banking	Bank Asia
20	Md. Kayser Hasan	Senior Manager, SME Banking Division	BRAC Bank

Annex Table 1: Campaign Launch event participant

Activity Title: Campaign Workshops
Description: Cybersecurity awareness and Digital Security best practices focused capacity building workshop attended by MSMEs from diverse sectors and sizes.

Workshop No	District	Place	Date	Collaborating Org.	Male	Female	Total Participants
1	Dhaka	SME Foundation Conference Hall, Dhaka	18/02/2023	SME Foundation	3	37	40
2	Dhaka	SME Foundation Conference Hall, Dhaka	28/02/2023	SME Foundation	27	0	27
3	Chattogram	CWCCI Conference Hall, Chattogram	11/03/2023	CWCCI	6	45	51
4	Chattogram	CWCCI Conference Hall, Chattogram	12/03/2023	CWCCI	5	39	44
5	Chattogram	CWCCI Conference Hall, Chattogram	13/03/2023	CWCCI	5	41	46
6	Cox's Bazar	Cox's Bazar Zilla Parishad, Cox's Bazar	29/04/2023	CYEC	7	15	22
7	Narayanganj	Ali Ahammed Chunka City Library and Auditorium, Narayanganj	04/05/2023	WE	2	63	65
8	Faridpur	Bel Piatoo	12/05/2023	WE	3	43	46
9	Khulna	Zilla Shilpokola Academy	26/05/2023	WE	16	110	126
10	Jashore	Hotel City Plaza	27/05/2023	WE	22	72	94
11	Dhaka	Shinepukur Suites	29/05/2023	e-CAB	21	5	26
12	Bogura	Hotel La Villa	04/06/2023	SME Foundation	46	13	59
				Total Participants:	**163**	**483**	**646**

Annex Table 2: Campaign Workshops List

Activity Title: Campaign Gambhira (Interactive Theatrical Performance)
Description: An interactive Theatrical Performance involving singing and dancing actors and singers through their performance disseminating crucial and most relevant Digital Security Best Practices to attendees.

Gambira No	District	Place	Date	Total Participants (Approx.)
1	Khulna	Badamtala Bazar, Batiaghata, Khulna	03/26/2023	160
2	Jashore	Sri-poddi Primary School, Jessore	03/27/2023	220
3	Bogra	Sherua Bottola, Sherpur, Bogra	04/07/2023	150

Annex Table 3: Campaign Gambhira List

Activity Title: Campaign Event Activations
Description: The campaign team visits different MSME Fairs and Events to disseminate awareness messaging and interact with the MSMEs present through different activities.

Date	Event Name	Type of Event	Event Size	Response Rate	Activities
14/12/2022	Connecting SMEs with IT Firms	Workshop	50 MSME Participants	50 MSMEs	- Introducing the campaign - Campaign website visited through QR code scanning - Assessment test taking through QR code scanning
30/12/2022	Online Community Management Event	Workshop	150 MSME Participants	150 MSMEs	- Introducing the campaign - Campaign website visited through QR code scanning - Assessment test taking through QR code scanning
23/01/2023	Ctg IT Fair '23	IT Fair	Stalls: 50+	50 MSMEs	- Introducing the campaign - Campaign website visited through QR code scanning - Assessment test taking through QR code scanning
19/02/2023	Ctg SME Trade Fair '23	MSME Fair	Stalls: 300+	200 MSMEs (Approx.)	- Introducing the campaign - Leaflet Distribution - Voxpop - Campaign website visited through QR code scanning - Assessment test taking through QR code scanning
14/04/2023	Sowda Hut	MSME Fair	Stalls: 25+	20 MSMEs	- Voxpop by Smita Chowdhury - MSMEs were added to the Campaign's Community Group - Campaign website visited through QR code scanning - Assessment test taking through QR code scanning

Annex Table 4: Campaign Events List

Annex-2: Online Activity Data

Activity Title: Social Media Campaign
Description: Disseminating awareness messaging regarding Cybersecurity through various creative content using social media platforms
Relevant Links: https://www.facebook.com/msmedigitalsafety
https://www.instagram.com/bebshaydigitalshurokkha/
https://bebshaydigitalshurokkha.com/

Sl.	Type of Content	Topics Covered	Social Media Channels	Content
1	Static Awareness-Based Content	**1.** Malware **2.** Phishing Scam **3.** Ransomware **4.** Insider Threats **5.** Online Supplier Scam **6.** Business page hacking and page fraud **7.** Fake delivery or fake address scam **8.** Fake payment	Facebook Instagram Campaign Website	84
2	Dynamic Awareness-Based Content		Facebook Instagram Campaign Website	20
3	Interactive Content	**9.** Strong Password Quiz **10.** Digital Hygiene Checklist Quiz **11.** MFS Scam Quiz **12.** Fake Offer/Scam Quiz **13.** Phishing link Quiz	Facebook	10
4	Influencer Collaboration	**14.** Cyber Preparedness Self-Assessment Test Promotion **15.** Campaign Workshop Promotion **16.** Campaign Event and Vox Pop Content	Facebook	3
5	2D Comic Strips	**17.** Malware, Phishing Scam, Ransomware, Insider Threats, Fake delivery or fake address scam, Fake payment	Facebook	9

Annex Table 5: Campaign Social Media Activity List

<table>
<tr><td colspan="5"><b>Activity Title:</b> Campaign Webinars
<b>Description:</b> Online events with various objectives that primarily involve key stakeholders of the campaign discussing different subject matters related to Cybersecurity, especially concerning MSMEs</td></tr>
<tr><th>Webinar No.</th><th>Webinar Title</th><th>Date</th><th>Total Participants (Unique)</th><th>Total Views on social media</th></tr>
<tr><td>1</td><td>How can MSME Entrepreneurs adopt Cybersecurity best practices?</td><td>12/12/2022</td><td>150</td><td>2,500</td></tr>
<tr><td>2</td><td>Digital Safety in Business: Women's Perspective</td><td>01/05/2023</td><td>1300</td><td>13000</td></tr>
</table>

Annex Table 6: Campaign Webinar List

<table>
<tr><td colspan="5"><b>Activity Title:</b> Campaign Live Q&A sessions
<b>Description:</b> Online live Q&A sessions by experts that primarily involve addressing the queries of participants of the campaign on matters related to Cybersecurity, especially concerning MSMEs</td></tr>
<tr><th>Webinar No.</th><th>Title</th><th>Date</th><th>Total Participants (Unique)</th><th>Total Views on social media</th></tr>
<tr><td>2</td><td>Weekly Digital Safety Q&A with Cybersecurity Experts 1</td><td>16/03/2023</td><td>60</td><td>800</td></tr>
<tr><td>3</td><td>Weekly Digital Safety Q&A with Cybersecurity Experts 2</td><td>23/03/2023</td><td>55</td><td>450</td></tr>
<tr><td>4</td><td>Weekly Digital Safety Q&A with Cybersecurity Experts 3</td><td>30/03/2023</td><td>75</td><td>1,300</td></tr>
<tr><td>5</td><td>Weekly Digital Safety Q&A with Cybersecurity Experts 4</td><td>13/04/2023</td><td>40</td><td>500</td></tr>
</table>

Annex Table 7: Campaign Live Q&A sessions List