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

ব্যবসায় ডিজিটাল সুরক্ষা

USAID FROM THE AMERICAN PEOPLE · DAI · DCCP DIGITAL CONNECTIVITY & CYBERSECURITY PARTNERSHIP · Inspira Advisory & Consulting