PLEXCONCIL

THE PLASTICS EXPORT
PROMOTION COUNCIL

दि प्लास्टिक एक्सपोर्ट प्रमोशन कौन्सिल
(भारत सरकार,वाणिज्य एवं उद्योग मंत्रालय,वाणिज्य विभाग द्वारा प्रायोजित)

THE PLASTICS EXPORT PROMOTION COUNCIL
(Sponsored By The Ministry Of Commerce & Industry, Deptt. Of Commerce, Government Of India)

Ref. No. :
Plexh/Cir/370 18.01.2021

To

All Members of the Council

Dear Sir/ Madam,

Subject: Regarding increased incidence of cyber fraud in international trade

Greetings from PLEXCONCIL!

This is to inform the members that there is an increased incidence of cyber fraud in international trade and that Indian exporters should be extremely cautious in doing business so that they don’t end up as victims.

Members are hereby advised to protect themselves from such cyber frauds by implementing security protocols like Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conformance (DMARC) as well as better password practices on both sender and receiver email IDs.

- SPF protocol based on the DNS of the domain name, certifies that the issuing IP has the right to send emails. This protocol is used to prevent fraudulent use of the domain name and prevents phishing attacks. It specifies which IP addresses and/or servers are allowed to send email “from” that particular domain. It lets the recipient know who has sent the communication.

- DKIM is a cryptographic protocol based on the use of public keys that are published in the DNS. It ensures that the content of emails remains trusted and have not been tampered with or compromised and the headers of the message have not changed and that the sender of the email actually owns the domain that has the DKIM record attached to it. The protocol allows the sender to sign the email with the domain name. The recipient of your email will then be sure that the email has been sent by the sender and has not been altered during transmission. This protocol is particularly effective against “man in the middle” attacks.

- DMARC provides indications in case there is an attack, ties the first two protocols (SKM and DKIM) together with a consistent set of policies. It is possible to be notified if someone tries to steal the identity of the sender. It verifies that a sender’s email messages are protected by both SPF and DKIM. It also tells the receiving mail server what to do if neither of those authentication methods passes, and provides a way for the receiving server to report back to the sender about messages that pass and/or fail the DMARC evaluation.

Members are once again requested to take adequate security measures as advised.

Regards,

Sribash Dasmohapatra
Executive Director
The Plastics Export Promotion Council
(Sponsored by the Ministry of Commerce & Industry, Govt. of India)
Dynasty Business Park, B Wing, Unit 2
Andheri East, Mumbai – 400 059
Ph: 91 22 4017 0000