Government of India
Ministry of Commerce & Industry
Directorate General of Foreign Trade
Udyog Bhawan, New Delhi – 110011

Dated: January 4th, 2021

Trade Notice No. 36/2020-21

To
All Export Promotion Councils
All members of the trade
All RAs of DGFT

Sub: Cyber fraud complaints from Indian Exporters - Trade Advisory -reg

Ministry of External Affairs has informed that email spoofing/phishing cyber frauds are causing increased bilateral trade disputes. Though this is registered as a cybercrime in the respective jurisdictions of the country, the authorities cannot do much to reverse the transaction. The victims end up being Indian exporters who having supplied the goods. They neither have the goods in their possession nor have received the payment.

2. The matter was examined and such problems can be largely resolved by implementing security protocols such as Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting & Conformance (DMARC). SPF, DKIM, and DMARC are protocols for standard email signatures which meet various safety issues and all three must be implemented in order to ensure the best possible deliverability. All three prove that the sender is legitimate, that their identity has not been compromised and that they're not sending email on behalf of someone else. They are all based on the Domain Name System (DNS) of the domain.

3. 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.

4. 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.

5. 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.

6. It is also suggested that better password practices be followed on both the sender's and the receivers' email IDs and to avoid this completely, exporters may like to confirm bank details by another channel such as a secure voice line.

7. EPCs/Traders are advised to take all precautionary measures to protect their payments from cyber frauds.

8. RAs are advised to inform trade as part of the outreach exercise.

9. This issues with the approval of the Competent Authority.

(Manoj Kumar Singh)
Joint Director General of Foreign Trade
Email: singh.mk@nic.in
Ph: 23061562 Extn: 343

(01/36/218/25/AM20/Coordination)