Subject: -

Cyber Security Advisory - Phishing Email Attack - IDEAS 2022 (Advisory No. 42)

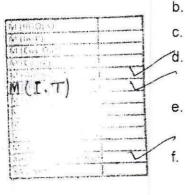
International Defence Exhibition and Seminar (IDEAS) is conducted by Defence Export Promotion Organization (DEPO). IDEAS-2022 is scheduled on 15-18 November, 2022 at Expo Centre Karachi. In this context, various fake emails pertaining to IDEAS/ DEPO have been received to various key appointment holders. Recently, a spear phishing email campaign with attached document IDEAS 22 Sponsorships.pdf has been observed. On clicking the document, it leads to a phishing page that asks for Gmail password. Analysis is attached as Appendix-I.

2. The situation warrants vigilance and adoption of preventive measures against spear phishing email attacks. All concerned are required to adopt a comprehensive email security and authenticity mechanism during correspondence. Few recommended best practices, but not limited to, against phishing emails are as follows: -

- Always be vigilant and ensure identity of sender. Do not click on link before verifying its sender.
- b. Never enter passwords without identifying link of website.c. Deploy a SPAM filter that detects viruses, blank senders, etc.
 - Keep all systems up-to-date with latest security patches/updates.
 - Always use an antivirus solution, schedule signature updates and monitor the antivirus status on all equipment.

Develop and implement an email security policy that is not limited to password expiration and complexity.

- g. Ask your system/ email administrator to deploy a web filter to block malicious websites.
- h. Ensure that all your email is effectively signed (DKIM) and verified on delivery (DMARC) to protect from attackers trying to send messages imitating to be originated from your domain.



3. Kindly disseminate the above message to all concerned in your ministries/ divisions/ departments including all attached/ affiliated departments and ensure necessary protective measures.

Appendix I

ANALYSIS OF PHISHING EMAIL - IDEAS 22 SPONSORSHIP.pdf

- 1. <u>Email Sender</u>. DEPO Pakistan (<u>so.epw@moib.gov.pk</u>)
- 2. Document. IDEAS 22 Sponsorships pdf
- 3. Email Details
 - a. Email contained a pdf document with a pushbutton image and malicious link. On clicking, it leads to malicious link with phishing page, asking for Gmail password. Generally, the attack campaign is of low-level and easily identifiable. Usually such links use Adobe Acrobat PDF.
 - b. The links embedded in phishing PDF files often take the user to a masqueraded website, from where user are redirected to a malicious website.
 - c. These phishing files do not necessarily carry a specific message, as they are mostly static images with a picture of a play button ingrained in them. Upon clicking the play button, user is redirected to another website.