

No.10(6)/2016-Coord
Government of Pakistan
Ministry of Science and Technology

Islamabad, 11th October, 2022

- | | | |
|--|---|--|
| 1. The Chairman,
PCSIR, <u>Islamabad.</u> | 2. The Director General,
NIO, <u>Karachi.</u> | 3. The Director General,
PSQCA, <u>Karachi.</u> |
| 4. The Chairman,
PSF, <u>Islamabad.</u> | 5. The Rector,
CU, <u>Islamabad.</u> | 6. The Director General,
NIE, <u>Islamabad.</u> |
| 7. The Chairman,
PCST, <u>Islamabad.</u> | 8. The Director General,
PNAC, <u>Islamabad.</u> | 9. The Rector,
NUST, <u>Islamabad.</u> |
| 10. The Director General,
PCRET, <u>Islamabad.</u> | 11. The Chairman,
CWHR, <u>Karachi.</u> | 12. The Chairman,
PEC, <u>Islamabad.</u> |
| 13. The Rector,
NUTECH, <u>Islamabad.</u> | 14. The Managing Director,
STEDEC, <u>Lahore.</u> | 15. The Director General,
PHA, <u>Islamabad.</u> |
| 16. The Managing Director,
NEECA, Islamabad. | | |

Subject: **CYBER SECURITY ADVISORY – PHISHING EMAIL ATTACK – IDEAS 2022 (ADVISORY NO.42)**

Please find enclosed herewith a copy of Cabinet Division's, Cabinet Secretariat (NTISB) Letter No.1-5/2003(NTISB-II) dated 4th October, 2022 on the subject cited above for information & compliance.

Encl: As above.


(HARIS BIN TARIQ)
Section Officer (Coord)
Tel: 9202520

Copy for information to:-

- i. PS to Secretary, MoST.
- ii. PS to Additional Secretary, MoST.
- iii. All heads of Wing's, MoST.
- iv. SO (Estt.), MoST.

**GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)**

No. 1-5/2003 (NTISB-II)

Islamabad, the 4th October, 2022

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: -

- a. 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.
- d. Keep all systems up-to-date with **latest security patches/ updates**.
- e. Always use an **antivirus solution**, **schedule signature updates** and monitor the antivirus status on all equipment.
- f. **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.


Dy No: 1828
SO (Coord):
Date: 11/10/22

SO (PA) Section
Diary No: 1243
Dated: 11/10/22

SECRETARY MOST
 6308
 6/10/22
 174.7893/DS(M)
 5-10/22
 JEA-1S11
 6-10-22
 5/11/UEA-III
 07/10-2022
 For compliance to orig circulation 25/10/22
 SO (Coord)
 DS/CA
 DE/II
 Cont'd...P/2
 SO (Coord)

Pl. circulate among all SFT org.
 07/10/2022
 7-70-22

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


(Muhammad Usman Tariq)
Assistant Secretary-II (NTISB)
Ph# 051-9204560

All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments

Copy to: -

1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-III, Cabinet Division, Islamabad
5. Director General (Tech), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad

Appendix I

ANALYSIS OF PHISHING EMAIL – IDEAS 22 SPONSORSHIP.pdf

1. Email Sender. DEPO Pakistan (so.epw@moib.gov.pk)
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**.