

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

Handwritten signature and initials in black ink, located at the bottom right of the page.

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.