F. No. 2(16)/2022-Misc-IT
Government of Pakistan
Ministry of Science & Technology
****

Islamabad, the 12th February, 2024

1. The Chairman, PCSIR, **Islamabad.**
2. The Chairman, PSF, **Islamabad.**
3. The Chairman, PCST, **Islamabad.**
4. The Chairman, PEC, **Islamabad.**
5. The Chairman, CWHR, **Karachi.**
6. The Rector, CUI, **Islamabad.**
7. The Rector, NUST, **Islamabad.**
8. The Rector, NUTECH, **Islamabad.**
9. The Director General, PNAC, **Islamabad.**
10. The Director General, PCRET, **Islamabad.**
11. The Director General, NIE, **Islamabad.**
12. The Director General, PHA, **Islamabad.**
13. The Director General, PSQCA, **Karachi.**
14. The Director General, NIO, **Karachi.**
15. The Managing Director, STEDEC, **Lahore.**

Subject: **FAKE EMAILS FORWARDED TO MINISTRIES/ DIVISION FROM E-MAIL ID OF JS (COORD).**

Dear Sir/ Madam,

Please find enclosed herewith a copy of self-explanatory letter No.1-3/2018-IT-12, dated 02nd February, 2024, on the subject cited above for information and compliance.

Encl: **As above**

(Kamran Nawaz Khan)
Deputy Electronics Adviser-I
051-9216304

Copy for Information to:
APS to JEA, MoST.

MOST IMMEDIATE

Government of Pakistan
Ministry of Information Technology and Telecommunication
DIGITAL PAKISTAN

F. No. 1-3/2018-IT-12 Islamabad the 2nd February, 2024

Subject: **FAKE EMAILS FORWARDED TO MINISTRIES / DIVISION FROM E-MAIL ID OF JS (COORD).**

Kindly refer to NTISB's letter number 1-5/2003/59/(NTISB-II) dated 6th October, 2023 on the subject cited above.

2 'Remedial Measures' (Annex-I) are forwarded herewith for information and compliance on priority basis.

3 Please detail a focal person (IT Official) to seek further guidance from Deputy Secretary, NTISB, Islamabad.

(Fakhira Akram)
Section Officer (IT)
Ph: 9215348

To all concerned Ministries / Divisions (Individually)

Copy for information.

1 PS to Secretary, MoITT, Islamabad
2 Secretary, NTISB Islamabad

REMEDIAL MEASURES

1. All the hard drives of infected systems should be isolated immediately.
2. Connect new hard drives to the systems, install latest registered windows. Update and install latest updates and drivers.
3. Cracked software should not be installed.
4. Install any highly reputed antivirus alongside windows defender. Install updates. And scan the whole computer.
5. Copy the required data from isolated hard drives without opening any file as per following:
    i. Do not paste any file that is in compressed archive, i.e. rar,7z,zip.tar etc. If necessary, copy the extracted file.
    ii. Paste only document files, i.e. doc, docx ,pdf, xls, etc.
    iii. Scan above files with updated antivirus.
    iv. Copy these files to new hard drives.
6. Block all the IOCs (Hashes, IPs, C&C) attached at **Appendix-I** (ATP Attack Files).
7. Block all the IOCs/Hashes for other detected malware.
8. Follow all the recommendations mentioned in NTISB's advisories.

Attachment View

Annex-MV: List of Malicious Files, hashes and their C&Cs

Sr. #	File Name	Hash	C&C
1.	PDF_Reader.exe	4c40fb701d962a7d068a316aeb297184	151.236.30.248
2.	PDF_Reader.exe	40705fee321427ed6de155dc72f56747	45.86.162.12
3.	msas.msi	7dc1d21554dce369586148l7e3f531e6	151.236.9.174 [Domain Name: Outlook.officeweb.live]
4.	Secur32.dll	c83a4eecb0a006792b1611a1b6e7b120	209.197.3.8
5.	gls.exe	d67fb0753c5af2655f6ce88264903f05	ftp://193.109.120.133:443
6.	Adobo_PDF.exe	e4ceb8b40863ecadc76f5db948546895	85.239.61:58
7.	gtsx.exe	f59e7138fe7c7d387cf3b5887a6e8279	ftp://194.36.188.9:443
8.	Dart.exe	98f6007dd8a18d14b03fa1bbf0b1e3a1	194.61.120.50:8080
9.	stx.exe	14ae82580b747636222cf570a4391968	188.119.149.201
10.	gog.exe	4b6b8135e2d48891c68cc66cd9934c40	
11.	Kashmir Solidarity Day 05.02.2023.doc	23516a147bca33113d55fee4c023252f	23.163.0.133
12.	2023 Military Awards.pdf.chm	e326777a34b1a752b662f8316cf588b3	Bbss.gov.pk
13.	Kashmir Report.rar | serp.exe	992e1ac3c087f0712c38787a96d4d430	151.236.30.248
14.	Notice 3rd meeting EC SIFC.rar	d6cfdbfa3992271dc8fcecdef3d0a852	-