

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

Islamabad, 19<sup>th</sup> December, 2022


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

Subject: **ADVISORY - CORPORATE BUSINESS AND TECHNOLOGIES  
OPERATING IN INDIA (ADVISORY NO. 52)**

**ii. CYBER SECURITY ADVISORY - LEAKAGE OF SENSITIVE DATA  
ON DARK WEB (ADVISORY NO. 53)**

Please find enclose herewith a copy of Cabinet Division's, Cabinet Secretariat (NTISB) Letters No. 1-5/2003 (NTISB-II) dated 14<sup>th</sup> December, 2022 on the subject cited above for information & compliance.

Encl: **As above.**

  
(SABED AHMED RAHOOJO)  
Section Officer (Coord)  
Tel: 9202520

Copy for information to:-

- i. PS to Secretary, MoST.
- ii. PS to Additional Secretary, MoST.
- iii. APS to Joint Secretary (Admn), MoST.
- iv. PA to Deputy Secretary (Admn), MoST.
- v. All heads of Wing's, MoST.
- vi. SO (Estt.), MoST.
- vii. Networking Administrator, MoST

GOVERNMENT OF PAKISTAN  
CABINET SECRETARIAT  
CABINET DIVISION  
(NTISB)

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

Islamabad, the 14 December, 2022

Subject:- Advisory - Corporate Business and Technologies Operating in India (Advisory No. 52)


Selected IBM software businesses (including Big Fix, Apps Can, Unica, Web Sphere, Lotus Nites, Domino and Tivoli) were acquired by M/s HCL Technologies Ltd, India in 2019. In this backdrop, NTISB has already shared an advisory vide this Division's letter No. 1-5/2003 (NTISB-II), dated 15 November 2019. However, despite lapse of over 3x years since HCL India acquired IBM solutions, SECP is still using HCL provided solutions online; posing a serious national cyber security concern.

2. Above in view, it is once again requested that all Federal Ministries, Divisions, Provincial Chief Secretaries, affiliated/attached departments, autonomous bodies, CMOs and ISPs to take following substantial measures:-

- a. Organizations using HCL provided solutions online (i.e. directly connected to internet) be advised to discontinue their use as soon as possible.
- b. In scenario, where organizations are using HCL procured solutions offline (i.e. in private networks and not connected with internet) may continue using these without applying and HCL provided update/patch/remote access etc. these organizations should procure alternate solutions as soon as possible suggested below: -

- (1) Microsoft System Center Configuration Manager (SCCM).
- (2) Kaspersky Endpoint Protection/Patch Manager.
- (3) Symantec Endpoint Protection/Patch Manager.
- (4) Window Server Update Services (WSUS).

3. Kindly disseminate the above message to all concerned in your organizations and ensure implementation.

  
(M. 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


ADDL SECRETARY MOST  
Dy. No: 7201  
Date: 15-12-22

Deputy Secretary (Admin)  
Dy. No: 7949  
Date: 16/12/22


S491  
15-12-22

JEA -1776  
15-12-22

DEATH/441  
16/12/2022

  
16/12/22  
DSCA

DEA fur  
19/12

  
15-12-22


14/3  
Date: 19/12/22

GOVERNMENT OF PAKISTAN  
CABINET SECRETARIAT  
CABINET DIVISION  
(NTISB)

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

Islamabad, the 14 December, 2022

Subject: - Cyber Security Advisory - Leakage of Sensitive Data on Dark Web (Advisory No. 53)

**Context.** Dark Web is part of WWW and is only accessible using distinctive software to allow users to remain anonymous or untraceable. It provides anonymity, protection from back-tracking and encrypted communication. Dark Web poses novel and formidable challenges to law enforcement agencies around the world.

2. **Dark Web versus Cyber Crimes.** Anonymity offered by Dark Web makes it a gateway to the world of crime and is known as hub of cybercrimes. Dark Web constitutes 96% of total data available on internet.

3. **Dark Web Access Techniques.** Access to dark web is managed by black market administrators. TOR browser (the onion route), I2P (invisible internet project), secure shell tool etc. are commonly used to access dark web. Nonetheless, explicit credentials are still needed to get unrestricted ingress to dark web forums.

4. **Use of Dark Web by Criminals.** Dark/deep web is being used by nefarious mindsets including criminals, terrorists, HIAS and non-state actors. Criminals are constantly inducting latest tools to enhance their attack weaponry. Few primary uses of Dark Web by criminals are as follows: -

- a. Digital crimes including hacking, cyber bullying/blackmailing, website defamation, buying zero day exploits/hacking tools, data dumps etc.
- b. Access to Personally Identifiable Information (PII) of citizens and key appointments via leaked databases.
- c. Scammed financial transactions via leaked banking/personal details.
- d. Honey pots to trap civilians and government organizations.
- e. Encrypted secure and private communication.
- f. Terror financing/money laundering and payments through cryptocurrency.
- g. Disseminating extremism, propaganda and publishing news of interest.
- h. Radicalization of potential targets.
- i. Terrorists' recruitments and trainings.
- j. Banned outfits' official statements on websites (anonymity of location).
- k. Cross border collaboration and terrorist support.
- l. Drug, human, obscene material and weapons trafficking.
- m. bounty hunting and ransom attacks.

5. **Recommendations.** Users are advised to put in efforts to protect personal and official data from being exposed to cyber criminals and further leakage on hacking forums/dark web.

In this regard, safety guidelines are mentioned in ensuing paras:-

- a. **Dark Web Guidelines**

Deputy Secretary (Admin) Addl. SECRETARY MOST  
 SECRETARY MOST  
 Dy. No. 5492  
 Date: 15-12-22  
 16/12/22

JEA-1777  
 15-12-22  
 DEA-1472  
 16/12/2022  
 19/12  
 DSCA  
 16/12/22

Dy No. 1412  
 SO (Coord)  
 Date: 19/12/22

15-12-22  
 15  
 15-12-22

- (1) Users are advised to stay away from exploring dark web sources (being unsafe)
- (2) Honey pots are already set up by HIAs and cyber criminals to trap civilians and government/intelligence organizations. Users should remain vigilant while surfing we.
- (3) Cyber criminals could exploit users/systems leading to hacking and leakage of personal/official data on dark web.

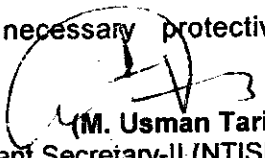
b. **Email/Social Media/Browser/other Apps**

- (1) Never forward, click/view link or pictures shared on email/WhatsApp by unknown sources/numbers.
- (2) It is mandatory to apply 2x factor authentication on all email, social medial and banking accounts.
- (3) One-Time Password (OTP) must never be shared with any one as it can compromise two-factor authentication.
- (4) Do not install untrusted software/applications (without digital signature) from third party sources on Windows and Android/iOS phone.
- (5) Do not install unnecessary plugins on browsers except Adblock and Adblock plus.
- (6) Always install and regularly update reputed antimalware/anti-virus solution on both Windows/Android phones.

c. **Mobile Phone Calls.**

- (1) All under command be sensitized not to share personal information, passwords or sensitive information on phone calls.
- (2) Vishing calls from unknown numbers must not be trusted and reported to PTA if found suspicious.
- (3) To counter social engineering/scam phone call, always ask relevant questions from caller and carefully judge him/her to ensure authenticity.

6. Kindly disseminate the above message to all concerned in your organizations, all attached/affiliated departments and ensure necessary protective measures.

  
(M. 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