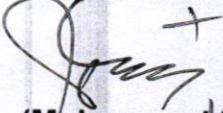


4. For any query or reporting malware/cyber incident, please forward the same on following email addresses: -

- a. Falcon1947@proton.me
- b. asntisb2@cabinet.gov.pk

5. Kindly disseminate the above message to all concerned in your organizations, 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 the Federal Government and Chief Secretaries of the 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

- (10) Always type URLs in browser rather than clicking on links.
- (11) Always open websites with https and avoid visiting http websites.

b. **Anti-Masquerading Guidelines**

(1) **Administrators**

- (a) Restrict incoming traffic and user's permissions to maximum extent by implementing system hardening at OS, BIOS and application level.
- (b) Unauthorized USB and storage media be blocked via hardening. Also, format USB every time before using to ensure no malware is propagated from one system to another.
- (c) Monitor networks including file hashes, file locations, logins and unsuccessful login attempts.
- (d) Use reputed anti-virus, firewalls, IPS/IDS and SIEM solutions.
- (e) Use separate servers/routing for offline LAN and online networks.
- (f) Allow internet access to specific users on need basis and restrict data usage/ applications rights.
- (g) verify software and documents before downloading via digital code-signing technique.
- (h) Implement MFA in mailing systems administrator controls and other critical systems.
- (i) Always maintain back up of critical data periodically
- (j) Regularly change passwords at administrator level
- (k) Regularly patch and update all OS, applications and other technical equipment.

c. **Users**

- (1) Always re-verify trusted user who has sent email/attachment via secondary means (call, SMS, verbal) before downloading.
- (2) Report any suspicious activity to Administrator immediately.
- (3) Never keep critical data on online systems and store it in standalone systems.