

8

GOVERNMENT OF PAKISTAN  
CABINET SECRETARIAT, CABINET DIVISION  
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD  
(NTISB-II)

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

Islamabad / 16 July, 2018

Subject: Advisory - Prevention Against Cyber Espionage (Advisory No. 137)

1. **Introduction.** Cyber has emerged as fifth dimension of warfare. Lack of security hardening at ISPs has made the Government **websites, email accounts** and **online services** a lucrative target of hostile agencies and continuously being hacked. Cyber Security of these organizations is matter of **national security** due to serious implications in case of any data breach.

2. **Implications.** Important ministries that are part of Critical Infrastructure if hacked may cause following effect on national security. Details are as under:-

- a. Compromised **email account** can be used for sending malwares to other official appointments.
- b. **Data of governmental** departments once hacked can be used by hostile elements for profiling and promotion of their agendas.
- c. **Compromised Data** can be used by non-state actors for carrying out subversion and anti-state activities.
- d. Comprised data can lead to **violation of civil rights of individuals** whose data have been leaked publically.

3. **Mitigation Measures for ISP.** Internet Service Providers (ISPs) may take following necessary measures for security of online data:-

a. **Cyber Security awareness of Employees**

- (1) All employees be given basic cyber security trainings.
- (2) All employees should be strictly ordered not to share any **official information/ passwords** with anyone else.

b. **Security of Devices.** Following best practices maybe adopted to ensure cyber security of devices, discussed:-

- (1) Always use strong password (uppercase, lowercase, special character) and change password in periodic fashion at least once every month.
- (2) To ensure security always follow the rule of **no default s tings.**
- (3) **Remote access** to admin panel should only be accessible via **VPN/** specific IP.
- (4) Regularly monitor logs of all devices for any suspicious activity.

c. **Security of Bandwidth**

- (1) **Dedicated firewall** should be deployed for all **sensitive users** of

**organization** and their traffic should be aggregated at one point.

- (2) Firewall policies should be properly configured to ensure best security practices.

d. **Security of Endpoint devices**

- (1) All endpoint devices e.g. Router given to end user should be managed centrally. User should not have any **rights** to access these devices i.e. telnet, ssh etc.
- (2) All devices should contain latest and updated version of **firmware**.

e. **Deployment of Security Devices**

- (1) Design and deploy security mechanism against **brute force** and **DDoS attack**.
- (2) Deploy **IPS/IDS** and firewall for security of digital infrastructure.
- (3) Deploy **web application firewall (WAF)** in case of online web services.

f. **Disaster Recovery Plan**

- (1) All services should be taken offline in case of any cyber incident.
- (2) There should be recovery plan in case of any cyber-attacks.
- (3) **Offsite Backup** should be maintained on daily and weekly basis.

4. **Security of Mail Server**

- (1) Enable TLS (enforcement) for secure email communication.
- (2) **DMARK, DKIM** and **SPF** record must be enabled.
- (3) Enable **SMTP** authentication to control user's access.
- (4) Enable **two factor authentication** for accessing webmail.
- (5) Enable per hour email sending limit.
- (6) Add legal footer, make sure that each email that is send out includes the necessary legal footer.
- (7) Block email with many recipients.
- (8) Delete the accounts of Ex- Employees/ unused email counts.

5. **Recommendations.**

- a. Regularly check the vendor website for updates and release of **security patches** of all operating systems/ softwares deployed.
- b. Approach Internet Service Provider (ISP) to strictly follow all mitigation measures at park 3.
- c. Carryout **penetration testing** and vulnerability assessment of all devices f security strength of servers and services.
- d. Hosting of email server on **shared hosting** is strictly **not recommended**. Approach service provider for confirmation of hosting details.

6. Forwarded for perusal and dissemination of information to all concerned, please.



Major  
(Ch Usman Firdous)  
Assistant Secretary -II (NTISB)  
Ph# 051-9204560

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