Priority

GOVERNMENT OF PAKISTAN
CABINET DIVISION
******

SUBJECT: CYBER SECURITY ADVISORY - REVAMPING CS POSTURE OF GOVERNMENT WEBSITES (ADVISORY NO.14)

Reportedly, various government websites of provincial departments (Baluchistan, Sindh and KPK) fell victim to defacement hacking attempts by adversaries during recent security environment. Initial analysis revealed weak CS posture of Govt websites and misconfiguration at administrator end. List of defaced websites (province-wise) is attached as **Annex-A**.

2. Such defacements merit attention to review overall CS posture of IT infrastructures and practices to identify and plugin vulnerabilities to avoid any cyber incident in the future.

3. Above in view, in order to rule out similar incidents in future, it is advised to approach concerned IT Boards/ Software Development Departments of Baluchistan, Sindh and KPK for sensitization/ implementation of best cyber security practices as deemed appropriate. In this regard cyber security best practices list is attached as **Annex-B**.

Annex-A

LIST OF DEFACED/HAKCED GOVT WEBSITES

Ser	Website	Province	PoC/Dept
1.	https://balochistan.gob.pk/	Baluchistan	Baluchistan IT Board (BITB)
2.	https://ipms.gob.pk/		
3.	https://aceb.gob.pk/		
4.	https://health.balochistan.gov.pk/		
5.	https://pw.balochistan.gov.pk/		
6.	https://balochistanhealthcard.gov.pk/		
7.	https://www.finance.gob.pk/		
8.	https://sindhculture.gov.pk/book.php?id=%27/%3cscript%20src=%22//jso-tools.zx.my.id/raw/-/dd9qvdjg3sq4m%22%3e%3c/script%3e	Sindh	Sindh IT Board (SITB)
9.	https://complain.kwsc.gos.pk/IBH.txt		
10.	https://steda.gos.pk/icm.html		
11.	https://www.steda.gos.pk/index.html		
12.	http://www.sindhlaws.gov.pk/		
13.	http://www.admission.hed.gkp.pk/colleqe.php?college_id=398	KPK	KPK IT Board (KPITB)
14.	https://cckb.edu.pk/		
15.	https://fts.kppolice.gov.pk/		
16.	https://swkpk.gov.pk/		
17.	https://assami.kp.gov.pk/		
18.	https://industries.kp.gov.pk/		
19.	https://mmdd.kpminerals.gov.pk/		
20.	https://www.kprts.gov.pk/		
21.	https://lgkp.gov.pk/		

NO. PS/DG-IIIS&ITD/OUTWARD/ 609 [redacted]
DATED: 06/8/25.

Annex-B

GUIDELINES FOR COMMUNICATION IT ASSESTS SECURITY

1. **Recommendations for Email Website Server Security**

a. **Use Strong Passwords**

(1) To ensure email security, always use strong passwords by employing combination of alphanumeric, special characters, upper and lower case letters.

(2) Avoid using general and easily guessable passwords e.g. DOB, own/ family names, vehicle registration number etc.

(3) Regularly change passwords.

b. **Avoid Email ID Exposure**

(1) Avoid sharing email ID with unknown persons.

(2) Always confirm the Identity of the individual to/ from whom email is being sent/ received.

(3) Avoid providing personal details in suspicious internet campaigns.

(4) Never use official email for private communication. Always use separate email IDs for personal and official correspondence.

(5) Never configure/ use official email on mobile phones.

c. **Be Aware of Phishing Attacks**

(1) Never open email attachments from unknown sources/ senders.

(2) If an email seems suspicious. Just ignore it; even don't try to unsubscribe by clicking unsubscribe link as it may allow hacker to access your emails data.

(3) Never open any attachment without anti-virus scan.

(4) If any suspicious email is received, immediately consult IT Administrator of your organization.

d. **Always Send Password Protected Documents**

(1) All email attachments sent must be encrypted with password.

(2) Password must be communicated through a separate channel such as SMS, Call or WhatsApp message.

(3) Delete password from the once received by the receiving party.

e. **Use Two Factor Authentication**

(1) In addition to strong passwords, also use two factor OTP via call/ message, password reenter mechanism etc.

(2) Never share your One Time Password (OTP) with anyone.

f. **Use Well Reputed and Licensed Anti-Virus**

(1) Endpoint (computer system or laptop) on which official email/ data is being ccessed/ sent must be secured through reputed; licensed and updated antivirus/ anti-malware solution.

(2) Always keep system firewalls activated and updated.

g. **<u>Use Robust Paid Anti-Spam Filters</u>**

(1) Use reputed Spam Filters.

(2) Do not rely on Google/ Yahoo's Spam Filters as email attackers have become much sophisticated.

h. **<u>Avoid Storing Data on Cloud Storage</u>**

(1) Never store personal and official data on cloud storage.

(2) Avoid using online document converting tools (Word to PDF etc) with cloud based data storage technology.

2. **<u>Cyber Security Measures - Websites Servers</u>**

a. Complete website/ server be deployed on inland servers including database and web infrastructure.

b. Detailed vulnerability assessment and penetration testing of application be carried out to identify potential threats.

c. Website/ server admin panel should only be accessible via white-listed IPs.

d. Proper security hardening of endpoints and servers be performed' and no unnecessary ports and applications be used.

e. Application and database be installed on different machines with proper system security hardening.

f. DB user's privileges be minimized and limited access be granted inside programming code.

g. Ensure network segregation through VLANs or physically (if deemed appropriate) in order to isolate online/ internet systems and offline/ official domains.

h. Implement data security/ protection protocols and solutions e.g. DEP CIEM, SOAR, IPSI IDS, Data Guard etc.

i. Sensitive data be stored in encrypted from with no direct public access.

j. Remote management services like. RDP and SSH must be disabled in production environment.

k. HTTP protocol be used for communication between client and web server.

l. Updated antivirus tools/ web application firewalls be used on both endpoints and servers to safeguard from potential threats.

m. Log retention policy must be devised for at least 3x months on separate device, for attacker's reconnaissance.

n. Enforce a strong password usage policy.

o. Email multi factor authentication must be ensured by sending an OTP to registered phone number only, in order to avoid any illegitimate/ unauthorized access to potentially sensitive data.

p. Defend websites against SQL injection attacks by using input validation technique.

q. Employ secure coding practices such as parameterized queries and proper input sanitization and validation to remove malicious scripts.

r. Regularly upgrade OS and webserver to latest version.

s. Keep system and network devices up to date

Major Hafiz Adnan Rana
Assistant Secretary NTISB-II
23 July , 2025, 11:53:08 AM

Major Hafiz Adnan Rana
Assistant Secretary NTISB-II

The Chief Secretary, Government of Sindh Karachi(Government of Sindh Karachi),
The Chief Secretary, Government of Balochistan(Government of Balochistan),
The Chief Secretary, Government of KPK(Government of KPK),
Cabinet Division No.1-5/2003/24(NTISB-II) Dated 29 July , 2025