SUBJECT: CYBER SECURITY ADVISORY - CISCO TALOS ANNUAL CYBER SECURITY ATTACK REPORT 2024 (ADVISORY NO. 10/2025)

Context. Recently, CISCO Talos has published annual cyber-attack report for 2024 covering various cyber security flaws linked to human negligence.

2. **Gist of Report**

a. Non implementation of cyber security best practices including MFA and strong passwords.

b. Weak implementation of Identity Control Systems allowed unauthorized access.

c. Usage of insecure VPN services created entry points for hackers.

d. Hackers used stolen credentials to gain unauthorized access of systems/apps.

3. **Advice for Users**. Above in view, a detailed cyber security advisory covering cyber best practices and safety guidelines is attached as **Annex-A**.

4. Kindly disseminate the above information to all concerned in your organization, attached/affiliated departments and ensure necessary protective measures.

JUL 2025
(Admin/HR)
.G (IT&DT)
.S (Rev. Div.)

Annex-A

CYBER SECURITY BEST PRACTICES AND SAFETY GUIDELINES

Introduction. In digital world, cyber space is increasingly vital to modern life, businesses and governments with the reliance on growing exposure to cyber threats and attacks. Non implementation of cyber security best practices continue to threaten the safety of cyber space. Strict implementation of cyber security best practices is essential to protect digital assets and privacy. Above in view, it is recommended to follow cyber safety guidelines proposed at para 2 & 3 to safeguard against hostile intrusions and sensitive data leakage.

F.n. 8, Please.

JUL 2025
C(IT)

2. **Recommendations for Email 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 letter.

SO(IT)

4. 7

(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 it 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 sending channel (SMS, WhatsApp etc) once received by the receiving party.

e. **Use Two Factor Authentication**

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

(2) Never share your One Time Password (0TP) with anyone.

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

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

(2) Always keep system Firewalls activated and updated.

g. **Use Robust Paid Anti-Spam Filters**

(1) Use reputed Spam Filters.

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

h. **Avoid Storing Data on Cloud Storage**

(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.

i. **Recommendations for Social Media Platforms, GSM and PDF Scanner**. Few guidelines (but not limited to) are as under:

(1) Do not share official documents via WhatsApp, Telegram, Messenger and other so called end-to-end encrypted messaging apps/secret chatting applications as their servers are hosted outside Pakistan.

(2) Do not use online PDF Scanner apps. Only scan secret documents via official hardened scanners.

(3) Do not discuss secret official matters on call/SMS/landline/GSM WhatsApp etc. Use officially dedicated communication numbers.

(4) Never store secret official documents in personal mobiles and PC.

(5) Do not store secret official documents in online systems. Always delete data after usage.

(6) Avoid using free and lucrative apps as majority of them steal data from PC and mobile phones.

(7) Do not use cracked versions of software. Always install paid software from official support and store.

(8) Ensure hardening of all online and offline official system.

j. **General Guidelines**

(1) Extreme caution be exercised on sharing sensitive data with vendors. Details, if required, to be shared must be obfuscated and shared on need to know basis.

(2) Public WiFi is more susceptible to attack as compared to private WiFi.

(3) Public WiFi Administrator might be monitoring network traffic and data sent online via internet packets.

(4) Passwords may be stored by network Administrator. Therefore, avoid using public WiFi for accessing personal/ official email.

(5) Regularly check and apply security updates.