URGENT

Priority

GOVERNMENT OF PAKISTAN
CABINET DIVISION
******

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. **Advise 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.

Please forward to all 7-7-25 DG-II

Please circulate immediately 7-7-25 DD(I).

Annex-A

CYBER SECURITY BEST PRACTICES AND SAFETY GUIDELINES

1. **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.

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.

   (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.

ED 07-7-25

(4) Never use official email for private communication. Always use separate email 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 (OTP) 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

(3) Do not discuss secret official matters on call/SMS/landline/GSM WhatsApp etc. Use 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 nes.

(7) Do not use cracked versions of software. Always install paid software from official support 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 hared 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 rnet packets.

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

(5) Regularly check and apply security updates.

Divisions of the Federal Government and Chief Secretaries of the Provincial Governments

Major Hafiz Adnan Rana
Assistant Secretary NTISB-II

CABINET DIVISION No.1-5/2003/24(NTISB-II) Dated 03 July, 2025

Priority

GOVERNMENT OF PAKISTAN
CABINET DIVISION

SUBJECT: CYBER SECURITY ADVIOSRY – USE OF SMART/IP TVS IN OFFICIAL PREMISES (ADVISORY NO. 11/2025)

In the light of current volatile cybersecurity landscape, it has been observed that adversaries are actively seeking to exploit unconventional attack vectors. Among these Smart TV and IP TV devices pose a serious cybersecurity risk, being equipped with microphone, camera, operating system and persistent internet connectivity. This offers, an attractive entry point for cyber attackers seeking to bypass traditional security parameters. Use of Smart TV and IP TV setups, serve as platforms for remote surveillance, network infiltration, malware propagation and unauthorized data exfiltration.

2. Apropos, Smart/ IP TVs installed/ being Used in conference rooms, Operations rooms, senior officer's offices and areas where sensitive work or information is being handled be immediately disconnected from internet and normal cable TVs be used instead.

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

Divisions of the Federal Government and Chief Secretaries of the Provincial Governments

Major Hafiz Adnan Rana
Assistant Secretary NTISB-II

CABINET DIVISION No 1-5/2003/24(NTISB-II) Dated 03 July, 2025

Priority

GOVERNMENT OF PAKISTAN
CABINET DIVISION
******

:T: FRAMEWORK FOR USAGE OF VPNS (ADVISORY NO. 12/2025)

Ministry of Interior has recommended PTA to develop a framework for responsible usage of VPNs as e their utility for legitimate purposes; VPNs are also identified by security agencies to be used for illegal oses including terror incidents.

2 In this regard, PTA is already providing facility to legitimate users (e.g. IT companies, business and rate entities, embassies, banks, freelancers), to register their VPNs for legitimate purposes through an online ss which is developed and streamlined as per the requirement of IT sector https://ipregistration.pta.gov.pk.

3. PTA has also commenced the licensing of Virtual Private Network (VPN) service providers under the License for the provision of Data Services in Pakistan. Complete list of Licensed VPN Service Providers in an are available at https://www.pta.gov.pk/category/list-of-operators-350607753-2023-05-30.

4. Kindly disseminate the above information to all concerned in your organization, attached/affiliated tments to ensure use of registered VPNs by PTA.

Divisions of the Federal Government and Chief Secretaries of the Provincial Governments

Major Hafiz Adnan Rana
Assistant Secretary NTISB-II

CABINET DIVISION No.1-5/2003/24(NTISB-II) Dated 03 July, 2025

Priority

GOVERNMENT OF PAKISTAN
CABINET DIVISION
******

SUBJECT: CYBER SECURITY ADVISORY - MALICIOUS SPEAR PHISHING EMAIL ATTACKERS (ADVISORY NO. 13/2025)

Context Reportedly, Indian threat actors are targeting government and defence departments for data acquisition via spear-phishing e-mails. In this regards, e-mails targeting specific users containing malicious documents have been identified. Details are as under:

2. **Modus Operandi**

a. Malware propagated via spear phishing file names related to Pahalgam Incident (UpdateOnPahalgamAttackIIOK).

b. The malicious file had an extension of **.chm** (Complied HTML), which when clicked executes a hidden executable/ malicious file in background

c. The malware after execution secretly collects data and images from device and further uploads to C&C (cyber espionage).

d. The documents contains screenshots of ARY, Duniya News, Channel 24, GTV, Express News etc. Details of malware are further elaborated in subsequent paragraphs.

3. **Technical/ Malware Details**

a. **Malware File Name**. UpdateOnPahalgamAttackIIOJK(1-4).chm

b. **Hidden File/ Malware Name**. UpdateOnPahalgamAttackIIOJK.exe

c. **File Extension**. chm (compiled HTML)

d. **Type of Malware** Infostealer Trojan

e. **Infection Vector**. Email, WhatsApp Messages

f. **Detection**. Highly evasive (currently no known antivirus can detect this)

g. **Prevention**. Apply system hardening controls

h. **Command and Control (C2 server)**.

Ser	IP Address	Port	Open Ports	Hosting Company	Location
(1)	151.236.21.48	8080	3386, 8080	M247 Europe (VPS Company)	France

i. Capabilities of Malware. Malware comprises of following capabilities:

(1) Querying of system information and account information including OS Name, OS Version, OS Manufacturer, OS Configuration etc

(2) The malware has the capability to query all system directions, shared folders, Documents, Downloads, Desktop and system drive and look for PowerPoint, Document files, Word and PDF files.

(3) The consolidated information/ documents are uploaded to C2 server mentioned in para systematic manner

4 **User Advice** Above in view, all users and administrators are advised to remain vigilant regarding phishing emails. Moreover, all administrators are advised to block above mentioned malicious domain/ URL on individual network firewalls. Cyber Security guidelines are attached as **Annex-A**.

5. For any query or reporting malware/ cyber incident, please forwarded the same on email address falcon1947@proton.me

6. Kindly disseminate the above information to all concerned in your organization, attached/affiliated departments for implementation.

Annex-A

CYBER SECURITY BEST PRACTICES - PREVENTION AGAINST CYBER -ATTACKS

Guidelines for Smart Phone/ Internet & Email Security

a. **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.

b. **Use Strong Passwords**

(1) To ensure email security, always use strong passwords 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.

c. **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 (OTP) with anyone.

d. **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 campaign.

(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.

e. **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

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 untrusted cloud storage.

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

Divisions of the Federal Government and Chief Secretaries of the Provincial Governments

Major Hafiz Adnan Rana
Assistant Secretary NTISB-II

CABINET DIVISION No.1-5/2003/24(NTISB-II) Dated 03 July , 2025