F. No. 3(5)/2023-NTISB-EW
Government of Pakistan
Ministry of Science & Technology
****

Islamabad, the 18th March, 2024

1. The Chairman,
PCSIR, **Islamabad.**

2. The Chairman,
PSF, **Islamabad.**

3. The Chairman,
PCST, **Islamabad.**

4. The Chairman,
PEC, **Islamabad.**

5. The Chairman,
CWHR, **Karachi.**

6. The Rector,
Comsats University,
Islamabad.

7. The Rector,
NUST, **Islamabad.**

8. The Rector,
NUTECH, **Islamabad.**

9. The Director General,
PNAC, **Islamabad.**

10. The Director General,
PCRET, **Islamabad.**

11. The Director General,
NIE, **Islamabad.**

12. The Director General,
PHA, **Islamabad.**

13. The Director General,
PSQCA, **Karachi.**

14. The Director General,
NIO, **Karachi.**

15. The Managing Director,
STEDEC, **Lahore.**

Subject: **Cyber Security Advisory – Fake Emails to Ministries/ Divisions (Advisory No. 04)**
Cyber Security Advisory – Dubious Adult Chat Applications (Advisory No. 05)

Dear Sir/ Madam,

Please find enclose herewith the subject advisories received from National Telecom and Information Technology Security Board (NTISB) Cabinet Division, for information and strict compliance.

Encl: **As above**

(Kamran Nawaz Khan)
Deputy Electronics Adviser-I
051-9216304

Copy for Information to:

i. APS to JEA, MoST.
ii. Network Administrator, MoST.

Circulate to all

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)

F. No. 1-5/2003/24(NTISB-II) Islamabad, the 8th March, 2024

Subject: - **Cyber Security Advisory - Fake Emails to Ministries/Divisions (Advisory No. 04)**

It has come to our notice that fraudulent emails purportedly originating from "JS (Coord)" are currently in circulation. These emails may contain malicious attachments or payloads aimed at compromising the security of our networks and systems.

2. All Ministries/Divisions and Government departments are urged to exercise caution and adhere to the following:

a. **Remain Vigilant.** Be cautious when receiving emails from both known/familiar sources such as "JS (Coord)" and unknown or suspicious sources. Scrutinize those requesting sensitive information or containing unexpected attachments.

b. **Verify Sender Information.** Verify the authenticity of the sender's emails address and domain. Pay close attention to any discrepancies or irregularities that may indicate fraudulent activity.

c. **Avoid Clicking Links or Opening Attachments.** Refrain from clicking on links or opening attachments from unfamiliar or untrusted sources. Malicious links or attachments may contain malware or phishing material designed to exploit vulnerabilities.

3. Please be advised that legitimate communications from "JS (Coord)" will originate from official government email addresses with appropriate domain extensions. Any deviation from these established channels should be treated with skepticism and reported immediately.

4. Kindly disseminate the above information 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

For ... r/.

DEA

JEA

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)

F. No. 1-5/2003/24(NTISB-II) Islamabad, the 8th March, 2024

Subject: - **Cyber Security Advisory - Dubious Adult Chat Applications (Advisory No. 05)**

This is in continuation of Cabinet Division NTISB's letter No. 1-5/2003/24(NTISB-II), dated 10th February, 2023 (Advisory No. 02).

Introduction. Sequel to already identified 120 x malicious apps, 12x new malicious apps are being used by the Hostile Intelligence Agencies (HIAs) for espionage/ information gathering. Newly identified applications are chat-cum-hacking apps used to trap civil and armed forces officials/personnel to extract classified information through technical/coercive (blackmailing) measures.

2. **Procedure to Uninstall the Apps**. Individuals who have accidently installed any of malicious apps mentioned in **Annex-A** must immediately perform the following actions:

a. Note down contact details (WhatsApp number/Facebook ID etc) of the suspected individual who shared the link for downloading the application for reporting the same to CSO of own organization/ department.

b. Immediately switch off infected mobile phone; remove battery (if removeable) & SIM and disconnect from internet.

c. Share this information/incident with known contact persons who have installed any of these apps.

3. **Recommendations.** Above in view, following best practices are recommended:

a. Always check application permissions before installation and install applications from the official application store only.

b. Under command should regularly be sensitized about malicious actors' tactics, techniques and procedures; moreover, all personnel (officers/ staff) be sensitized to refrain from engaging in activities that may lead to exploitation.

c. Install and update reputed antivirus solution on mobile devices like AVAST or Kaspersky. After installation, scan the suspected device with antivirus solutions to detect and clean infections.

d. Before downloading/ installing apps on Android devices, review the app details, number of downloads, user reviews/ comments and "ADDITIONAL INFORMATION" section.

e. In mobile settings, do not enable installation of apps from "Untrusted Sources".

f. Install OS updates and patches as and when available from device vendors.

g. Do not download or open attachment in emails received from untrusted sources or unexpectedly received from trusted users and immediately report to concerned office.

h. Avoid using insecure and unknown Wi-Fi networks as hostile elements use Wi-Fi access points at public places for distributing malicious applications.

i. Use two-factor authentication on all Internet Banking Apps, WhatsApp, Social Media and Gmail Accounts.

j. All officers/staff must be guided to adhere recommended cyber security measures at personal smart appliances.

4. Kindly disseminate the above information 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. Principal Secretary to the PM, Prime Minister's 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

Annexure A

LIST OF IDENTIFIED MALICIOUS APPLICATIONS

(As on 27 Feb 2024)

Ser	Malicious Appl Name	Ser	Malicious Appl Name	Ser	Malicious Appl Name
1.	Rocket Chat	2.	Safe Dialler	3.	Phub
4.	Omegle	5.	U & Me	6.	Babble V3
7.	Privatechat1	8.	Filos	9.	Chat It
10.	Rapid Chat	11	YoTalk	12.	Porn Hub
13.	Photo Edition	14.	Crypto Chat	15.	TeleChatty
16.	ZoIPER	17.	Babble	18.	Face Call
19.	Buzz	20.	Tweety Chat	21.	VIBES
22.	Converse	23.	Lite It	24.	Hex Chat
25.	Xpress	26.	Chat On	27.	Vmate
28.	Chirrups	29.	Link Up	30.	Safe Chat
31.	Graphic Version	32.	Secure Chat	33.	Lite Chat
34.	Pvt Chat	35.	Guftagu	36.	Cheerio
37.	Free VPN V3	38.	Twin Me	39.	Philions Chat
40.	Just You	41.	CuCu Chat	42.	FM WhatsApp
43.	Quran.Apk	44.	Fruit Chat	45.	Islamic Chat
46.	SecureIt	47.	ZanigV4	48.	Spitfire
49.	FaceChat	50.	Seta / SA News	51.	Wire
52.	FireChat	53.	Cable-1	54.	Privee Chat

Ser	Malicious Appl Name	Ser	Malicious Appl Name	Ser	Malicious Appl Name
55.	Buddy Chat	56.	Stumped	57.	Zong Chat (Beta)
58.	ZangiV2	59.	Media Services	60.	CrazyChat
61.	Chat 24/7	62.	Zapme	63.	Chat Pt
64.	Kakao Talk	65.	ZongBoost	66.	Audio & Video Recorder
67.	ISPRNews	68.	Love Bae	69.	Easy Chat
70.	Zepp	71.	Boss	72.	ChitChat Box
73.	Hideme	74.	Skymate	75.	Triover
76.	Peppyz	77.	LionVPN	78.	Paigham Chat
79.	Friend Chat	80.	Pink WhatsAp	81.	Dosti Chat
82.	Star Talk	83.	Gossip	84.	Mobile Chat
85.	Click (aval on Goggle Play store)	86.	Yooho Chat	87.	Howdee (aval on Goggle Play store)
88.	Pryvate	89.	Exodus	90.	TalkU
91.	Pakistani Mili Naghmee	92.	Ab Talk	93.	Text on Photos
94.	Pakistani Chat Rooms	95.	Imo	96.	Stripchat X
97.	Text on Photos	98.	Skype Lite	99.	Woo Plus
100.	Intimo	101.	Chat Privacy	102.	Android Services
103.	Android System Services	104.	Im Secure Chat	105.	Bigo Live Lite
106.	Live Chat Video Call-Whatslive	107.	MeetU	108.	Milli-Live Video Call
109.	JOJOO-Live Video Chat	110.	Gibber-Live Video Chat	111.	BunChat Pro Video Chat
112.	iBlink-Live Video Chat	113.	Online Live Adult Video Chat	114.	Video Chat With Strangers

Ser	Malicious Appl Name	Ser	Malicious Appl Name	Ser	Malicious Appl Name
115.	Charm-Match with Singles	116.	Sexy Girl Video Call	117.	XV Random Video Chat
118.	Bubble for chat	119.	18Live: Live Random Video Chat	120.	Live Talk Video Call
121.	Privee Talk	122.	YohooTalk	123.	TikTalk
124.	MeetMe	125.	Let's Chat	126.	Quick Chat
127.	Rafaqat	128.	Chit Chat	129.	Hello Chat
130.	Glow Chat	131.	Nidus	132.	Wave Chat