



FAX: 051-9250746

REGISTERED A/D  
MOST IMMEDIATE

No. PEN-8[5]/2017

2899

GOVERNMENT OF PAKISTAN  
CABINET SECRETARIAT [AVIATION DIVISION]  
PAKISTAN METEOROLOGICAL DEPARTMENT

Islamabad, the 22nd December, 2017.

To: Wafaqi Mohtasib [Ombudsman]'s Secretariat,  
36-Constitution Avenue, G-5/2,  
Opposite Supreme Court,  
Islamabad.  
[Kind Atten: Hafiz Ahsaan Ahmad Khokhar, Senior Advisor [Law]/Grievance Commissioner for  
Overseas Pakistanis].

SUBJECT: MEETING HELD AT WAFAQI MOHTASIB SECRETARIAT, ISLAMABAD ON NOVEMBER 8, 2017 TO  
REVIEW IMPLEMENTATION OF INSTRUCTIONS/GUIDELINES FOR ESTABLISHMENT OF PENSION  
CELLS AND PENSION FACILITATIONS INITIATIVES IN MINISTRIES/DIVISIONS/DEPARTMENTS ETC.

Dear Sir,

I have the honour to invite a reference to Wafaqi Mohtasib Letter No. 4[7]/IMPL. Report/EPCRM/SL/WMS/2016 dated 13-11-2017 and to assure that this office is making all out efforts to ensure early disposal of each pension case and Focal Person of PMD is also maintaining constant oversight. A statement containing necessary information on the prescribed format about disposed off pension cases in the month of December, 2017 is enclosed as desired.

2. This issue with approval of DG Mets.  
[As Above].

Your's faithfully;

[MUHAMMAD ARIF]  
Deputy Chief Admin. Officer  
For Director-General  
Meteorological services.  
Ph: 051-9250677

Copy To:

1. Mr. Waqar Zulfiqar Ahmed Asif, Section Officer [Admin], Cabinet Secretariat [Aviation Division], Islamabad with-reference to Letter No. 5-54/Admin-2014 dated 20-11-2017.
2. Chief Meteorologist [Focal Person], NDMC, Islamabad.
3. Mr. Zeeshan Haider, Programmer, NDMC, Islamabad to upload the details on PMD's website. The detail may please be seen at your hotmail address.

1085

GOVERNMENT OF PAKISTAN  
PAKISTAN METEOROLOGICAL DEPARTMENT  
(HEADQUARTER OFFICE)  
P. O. BOX NO.1214, SECTOR H-8/2,  
ISLAMABAD

No. GA-21(46)/2013 *2948*

Islamabad, the *26* Dec. 2017

CIRCULAR

Subjects: ADVISORY – PREVENTION AGAINST MICROSOFT SECURITY FLAWS (ADVISORY NO. 94).

ADVISORY – PREVENTION AGAINST FAKE WHATSAPP ON GOOLE PAY STORE (ADVISORY NO. 97 DATED 13- NOV. 2017).

ADVISORY – PREVENTION AGAINST CYBER EXPIONAGE (ADVISORY NO. 98).

Kindly find enclosed herewith a copies of National Telecom & Information Technology Security Board, letter No. 1(5)/2003(NTISB) dated 15<sup>th</sup> & 30<sup>th</sup> Nov. 20127 on the above subjects for information and further necessary action.

Encl: (As above)

  
(ALLAUDDIN)  
SUPERINTENDENT

Distribution:-

1. Chief Met., Drought / R&D, Met. HQs. Office, Islamabad.
2. Chief. Met, FFD, Lahore / Karachi.
3. Director, RMC, Karachi / Lahore / Peshawar / Quetta / GB.
4. Syed Zeeshan Haider (Programmer) Please upload on PMD's Website.

} Through PMD website

P-1411

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

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

Islamabad 30 November, 2017

**Subject: Advisory — Prevention Against Cyber Espionage (Advisory No. 98)**

1. **Introduction.** A critical vulnerability of TOR browser has been identified by Italian security researcher Filippo Cavallarin. This vulnerability can leak real IP addresses of users to potential attackers, upon visiting certain types of web page.

2. **Affected Software.**

- a. The vulnerability affects Tor browser for mac OS and Linux. However it doesn't affect Windows users apparently.
- b. This vulnerability would affect the privacy and security of Tor users.

3. **Mode of operation.** Mode of operation is as under:-

- a. The vulnerability resides in Firefox that also affects Tor Browser, as the privacy-aware service that allows users to surf the web anonymously uses FireFox at its core.
- b. **TorMoil** bug, the vulnerability affects Tor browser. TorMoil is triggered when users click on links that begin with file:// addresses, instead of the more common https:// and http:// addresses.
- c. Once an affected user [running macOS or Linux system] navigates to a specially crafted web page, the operating system may directly connect to the remote host, bypassing Tor Browser

4. **Recommendations.** Following is suggested in this regard:-

- a. The Tor Project has currently issued a temporary workaround to prevent the real IP leakage.
- b. MacOS and Linux users may find the updated versions of the Tor anonymity browser that will not behave properly while navigating to file:// addresses, until a permanent patch becomes available.
- c. Regularly update the system with latest anti-virus.
- d. Update TOR to version 7.0.8.
- e. **Install and UPDATE well reputed antiviruses** such as Kaspersky, Bitdefender, Nod 32, Avast etc.
- f. Update all softwares including Windows OS, Internet browser (Mozilla, Firefox) and Microsoft Office.
- g. Install and regularly update software firewall such as Comodo Firewall or ZoneAlarm.

Aviation Division  
 Section Officer (Admin)  
 Diary No: 1955 Date: 6-12-17  
 Deputy Secretary (Admin)  
 Diary No: 2572 Date: 07-12-17  
 Joint Secretary-III  
 Diary No: 2878 Date: 27/12

By. No. 5582	SECY	
DATED: 26/11/17		
III-SK	Sr. JS-II	Sr. JS-I
✓		

~~SECRET~~

SECRET

MA 28/12  
DS (Admin)  
(ATL)  
S.O (A)



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

Islamabad 30 November, 2017

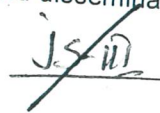

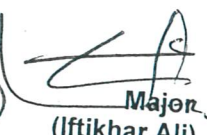
**Subject: Advisory -Prevention against Fake WhatsApp on Google Play Store (Advisory No. 97 Dated 13 Nov 2017)**

AVIATION DIVISION  
 Section Officer (Admin)  
 Diary No. 124 Date 8-12-17  
 AVIATION DIVISION  
 Deputy Secretary (Admin)  
 Diary No. 2573 Date 7/12  
 AVIATION DIVISION  
 Joint Secretary-III  
 Diary No. 2826 Date 07/12

1. **Introduction.** Google Play Store is surrounded by hundreds of fake and malicious apps that trick users into downloading and installing them and potentially infect their smart phones to carry out malicious things without their knowledge. Recently, a fake version of the most popular WhatsApp messaging app for Android has been spotted by some users. The app named **Update WhatsApp Messenger** was uploaded on the official Google Play Store by an app developer who pretended to be the actual WhatsApp service with the developer title "WhatsApp Inc."—the same title the actual WhatsApp messenger uses on Google Play.
2. **Technique Used.** The app developer was able to use the same title as the legitimate maker of the WhatsApp by adding a Unicode character space after the actual WhatsApp Inc. name, which in computer code reads **WhatsApp+Inc%C2%A0**. This hidden character space at the end of the WhatsApp Inc. was invisible to an average Android user browsing Google Play Store, allowing this dodgy version of the app to masquerade as a product of WhatsApp Inc.
3. **Mode of Operation.** The app once downloaded will perform following actions:-
  - a. Serve Android users with advisements to download other apps.
  - b. The app will try to hide by not having a title and having a blank icon.
4. **Recommendations.** In order to prevent user's data from being vulnerable to theft, the following is suggested.
  - a. Vigilantly download apps not only from the third-party app store but also from official Play Store in order to protect yourselves.
  - b. Backup your files regularly.
  - c. Scan system regularly with antivirus such as Kaspersky, Avira , Avast, ESET etc.
5. **Reporting of Suspicious Files/ Emails.** Any malicious email/file may be reported to this organization on the following email addresses for analysis and suggesting mitigation measures:-
  - a. eagle1978gmail.com
  - b. falcon098@writeme.com
6. Forwarded for perusal and dissemination of information to all concerned, please.

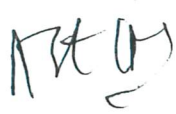
Copy No. 983 SECY  
 DATED: 08/12/17

III-SC	Sr. JS-II	Sr. JS-I
✓		

  
 (AOL) S.g.(A)  
 Major (Iftikhar Ali)  
 Assistant Secretary (NTISB)

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

**SECRET**

MA 08/12  


**SECRET**

- e. Install well reputed firewall with built-in HIPs (Host Intrusion Prevention System).
5. **Reporting of Suspicious Files/Emails.** Any malicious activity may be reported to this organization on the following email address for analysis and suggesting mitigation measures:-
  - a. eagle1978@mail.com
  - b. falcon098@writeme.com
6. Forwarded for perusal and dissemination of information to all concerned, please.



Major  
(Iftikhar Ali)

Assistant Secretary (NTISB)

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