

**GOVERNMENT OF PAKISTAN  
REVENUE DIVISION  
FEDERAL BOARD OF REVENUE  
(IT WING)**

\*\*\*\*\*

**SUBJECT: CYBER THREAT –FAKE MESSAGES / LINKS (ADVISORY NO. 80)  
CYBER SECURITY ADVISORY – APPLE THREAT NOTIFICATION  
AGAINST STATE SPONSORED (ADVISORY NO. 80)**

I am directed to forward the copies of the advisories received from National Telecom & Information Technology Security Board bearing even No.1-5/2003(NTISB-II) dated 3<sup>rd</sup> December, 2021 and 07<sup>th</sup> December, 2021 on the subject, for taking precautionary measures as advised in the letter and for uploading on FBR's Website.

**Encl:** (As above)

  
(Sajid Raza Mirza) 23/12/21  
Second Secretary (IT-I)

**Chief (FATE), Federal Board of Revenue (HQ), Islamabad.**

IT Wing's U.O.No.1(106)SS(IT)/2020-ADV/ 209518-R Islamabad the 23<sup>rd</sup> December, 2021

**GOVERNMENT OF PAKISTAN  
CABINET SECRETARIAT, CABINET DIVISION  
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD  
(NTISB)**

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

Islamabad 07 December, 2021

Subject: Cyber Security Advisory – Apple Threat Notification against State Sponsored Cyber Attack (Advisory No.80)

**Context** Recently, apple has generated alerts to inform its user who have likely been targeted by NSO Pegasus software. Apple threat notifications are designed to inform and assist users who have been likely targeted by state-sponsored attackers; however, Apple has not disclosed the means of identification of users which have likely been targeted. In this regard, Apple has already issued updates to counter the threat and sued Israeli company NSO for attacking iOS users.

2. **Apple Information Dissemination Mechanism.** Apple activity monitors its own manufactured devices for signs of compromise. In the recent event, Apple has informed its customers by following mechanism: -

- a. iMessage
- b. Email
- c. Alert on apple ID ([appid.apple.com](http://appid.apple.com))
- d. An apple user can check the validity of iMessage by visiting [appid.apple.com](http://appid.apple.com). The presence of message at [appid.apple.com](http://appid.apple.com) will prove legitimacy of iMessage.

\*

3. **Recommendations / Security Steps for users.** Above in view, users are requested to adopt following measures: -

(IP- Ops)	
(HR-P)	
(Cus-Ops)	
(Cus-P)	
(Admn/HR)	
(IT)	
(FATE)	
(Legal)	
(Reforms)	
(Legal & Acc. Cus)	
(Acc & Audit)	
(IT Secv (Rev. Dis))	
(IT Secv)	

- a. Immediately upgrade to iOS 15.1 or iOS 15.1.1 (for iPhone 12 or above) which covers security update related to above mentioned attack.
- b. It is advised to protect devices with strong passcodes and use two factor authentication on Apple ID.
- c. Install apps from official Apple Store only to avoid malware / infection.
- d. Use anonymity based solutions (over internet while surfing) and mask identity of key appointment holders / individuals.
- e. High ranking officials should not purchase phones / SIMs / internet devices on their own names / CNIC numbers / thumbprint.
- f. In phonebook / contact list, never save contacts with ranks / appointments / organization name etc with individuals' names.

FBR e-DOX Dy.No. 2021/285-R  
 Received in Chairman's Sectt  
 on 08 DEC 2021

*[Handwritten signatures and initials]*  
 13/12/21


*Secy (IT)*  
*chief (Systems)*

*SSC (IT)*  
*Received on 21-12-21*  
*Please put up today*  
*Assistive*  
*21/12/21*  
*(19)*

- g. Official identity should never be revealed and sensitive information should never be shared through phone.
- h. Always disable location from Apple devices.
- i. Strictly avoid using phone at sensitive locations / meetings.

4. **Reporting of Suspicious Files / Emails** Any malicious activity may be reported on following email address for analysis and suggesting mitigation measures: -

asntisb2@cabinet.gov.pk

  
Major  
(Muhammad Usman Tariq)  
Assistant Secretary-II (NTISB)  
Ph# 051-9204560

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

Copy to: -

1. Secretary to the Prime Minister, Prime Minister 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



**GOVERNMENT OF PAKISTAN  
CABINET SECRETARIAT, CABINET DIVISION  
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD  
(NTISB)**

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

Islamabad 3<sup>rd</sup> December 2021

**Subject: Cyber Threat – Fake Messages / Links (Advisory No. 80)**

1. Malicious actors are sending suspicious links masqueraded with tinyurl/bit.ly or sometimes a valid URL pointing to some malicious link. Therefore, it is requested not to open / click such links.

2. Disseminate the same message in your organizations, all attached / affiliated departments and ensure necessary protective measures. For any query or reporting malware, please forward the same on following email address: -

M (IR-Ops)	
M (IR-P)	
M (Cus-Ops)	
M (Cus-P)	
M (Admn/HR)	✓
M (IT)	✓
M (FATE)	
M (Legal)	
M (Re-former)	
M (Legal & Acc. Cus)	
M (Acc. & Audit)	
and Secy (Rev.Div.)	✓
... / SPS	

**asntisb2@cabinet.gov.pk**

*[Handwritten signature]*

**Lieutenant Colonel  
(Kamran Rashid)  
Deputy Secretary (NTISB)  
Ph# 051-9204560**

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

**Copy to: -**

1. Secretary to the Prime Minister, Prime Minister 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

*Forwarded to PRA*

*Secy (IT)*

*SS (IT-i) recd on 21-12-21  
R put up today*

BR #00X Dy.No. 202238R  
Received in Chairman's Sectt  
on 06 DEC 2021

*[Handwritten initials]*

*13/12/21  
Chief (Systems) - Assistant*