PS TO CMEF SECRETARY SINDH 18
Diary No. 33545
Inward Date 6/12/2018
Outward Date

NO. PS/SECY/I.T/1258
Dated: 6th 12-2018

DG IS&TD Dairy No. 1024
Dated 7-12-2018

GOVERNMENT OF PAKISTAN
CABINET SECRETRIAT, CABINET DIVISION
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB-II)

No. 1-5/2003 (NTISB-II) **Islamabad 30 November 2018**

Subject: **Advisory - Prevention against Cyber Espionage (Advisory No. 164)**

1. **Introduction.** In last decade, the use of smart TV has increased immensely. Recently, Security researchers have disclosed that along with advance features and service like reading emails, installing applications, surfing web etc, it is presenting a new attack vector to hackers for compromising and stealing sensitive information.

2. **Threats Posed by Usage of Smart TV.** Multiple studies dealing with security and privacy issues in smart TVs indicate following threats:-

   a. A Malware can easily find its way into smart TVs that could convert them into bugging devices.

   b. User profiling can be done by viewing logs , browsing history etc.

   c. Access to sensitive files, photos and other data on storage devices connected to your smart TV.

   d. Smart TV may become part of a botnet that can be used to attack corporate or government websites.

   e. Hackers can access the apps installed on the TV by user and steal personal / accounts information.

   f. These devices also come with a variety of out date firmware's and vulnerable applications.

   g. Smart TVs equipped with remote controls for voice commands and cameras for video conferencing making them the perfect tools for espionage.

   h. Hackers may lock the TV and demand a ransom.

   Continuous pop-ups with targeted advertisement.

Under CS Directive
For Perusal and
n/a pl.
PS TO CS
06/12/18
Sqn. Ldr. (I.T) GAIC

3. **Best Practices for safe Usage of Smart TV.** Following best practices may be employed for safe usage of smart TV:-

   a. Smart TV users are strongly advised to keep these devices off the network and ensure that the USB ports are not exposed.

For circulation pls
7/12/18
DG
7-12-18
DW 390 10-12-18
DD (IT) 10/12

b. Users are advised regularly install updates on the home TV as these updates may contain critical security fixes.

c. For pool proof security of webcam and / or microphone, cover them with opaque tape or a sticky note.

d. Limit online activity on smart TV, if required to log into banking website, never use TV instead use your phone or personal computer.

e. Be cautious when installing new apps and only install apps form known sources.

f. Set up a separate Wi-Fi account for your smart TV as hackers may reach your laptop or computer via your smart TV.

g. Avoid connecting USB sticks to the TV because they might contain malware.

h. Make sure your clearly understand the terms and conditions and privacy polices before activating any services on your smart TV.

i. It is also suggested to avoid using generic browsers on smart TVs because they don't have built-in security controls to protect against malicious web attacks

j. The old Wired Equipment Privacy (WEP) protocol is still widely used, but it is weak and easily compromised. Make sure the home wireless network is protected by Wi-Fi Protected Access II (WPA2) protocol and a, complex password.

k. Disable guest network access entirely.

l. Good password management is essential. Neither network equipment (such as routers and switches) nor gadgets (such as smart TVs) should use default factory -set administrator passwords.

m. Permanently disable remote - management access and other network tools.

4. **Recommendations.**

a. Smart TV are relatively new to the security field , as long a s manufacturers step up their cyber security and offer effective security features and strong firewalls , it is strongly advised to follow the guidelines outlined at Para 3.

b. Only purchases smart TVs from reputable vendors that have a track record of regularly fixing bugs and releasing security updates.

c. Keep all operating systems, firmwares and software up to date.

5. Forwarded for perusal and dissemination of information to all concerned, please.

Major
(Ch Usman Firdous)
Assistant Secretary-II(NTISB)
Tel#051-9204560

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

1. SPS to Cabinet Secretary , Cabinet Division Islamabad
2. PS to AS-III , Cabinet Division Islamabad
3. APS to Secretary, NTISB
4. APS to Deputy Secretary , NTISB