No. 350 Camp/2017-ID
Office of the
District Police Chief
Idukki. dated 01.07.2017.

From

District Police Chief
Idukki.

To

Administrative Assistant,
District Police Office,
Idukki.

Sir,

Sub : Ransom ware attack – precautionary measures – instruction issued- reg.

Your attention is invited to the subject cited above.

Lot of online intrusions are being reported into the computer networks of various offices, including Police offices across the state. In these circumstances, following instructions are issued with, for the safety of the computer network that is being installed in the District Police Office, Idukki.

1. Usage of pen drives and external Hard disks can disseminate viruses in a great deal. Hence they should not be plugged to the ports of the computers that being used in the DPO. However, since data transfer cannot be interrupted, staffs can make use of the internal messaging facility of iAPS, for transferring files for official use.
2. No private networks should be used in the official computers through WIFIs, Net setters, VPNs etc. KSWAN should only be used to access internet in DPO since it is equipped with enough security and Firewall settings. Even BSNL broadband connection is not advisable.
3. Mobile phones should not be tethered to the official computers.
4. Private Email IDs should not be opened from the official computers.
5. Software other than that for routine duties may not be installed in the computers. In case if any such software is necessary, contact Cyber cell or DCRB computer cell before installation, to ensure the safety.

6. Do not share files in between the computers in DPO using file sharing option.
7. All staffs should ensure that the computers used by them are being installed with genuine and updated windows version. Security patches are to be installed as and when it is available on network. This should be ensured in liaison with DCRB computer cell or Cyber cell.
8. In case if anything abnormal found in the functioning of the computers, it should be informed to the DCRB computer cell or Cyber cell and should be rectified then and there.
9. All the computers in DPO are installed with antiviruses like **Microsoft Security Essential** and **windows defender.** Every staffs should ensure their computer have an updated antivirus version. This can be ascertained easily by clicking the antivirus icon placed in the right bottom of the screen.
10. For backing up files, make use of iAPS or official mail system. It is safer to keep the files online than saving in the hard disks.
11. One computer should be set apart for accessing Email services. Emails received are to be printed out from that computer itself or passed on through iAPS making use of that computer itself.
12. In case if any technical difficulty is experienced, contact Cyber Cell or DCRB computer cell.
13. Cyber Cell and DCRB Computer cell should ensure the safety regarding this. They should make periodic checkups in the computers for ensuring safety.
14. All the aforementioned instructions should be strictly adhered to. Manager should personally ensure whether the instructions are complied with and should report if any dereliction is noted. Any negligence noted will be viewed seriously and will attract disciplinary actions.

District Police Chief
Idukki.

Copy to : The Manager, DPO Idukki
: DySP DCRB
: SI Cyber Cell