Subject:- **Prevention Against Ransomware (Advisory No. 10) June 2015**

Introduction. Ransomware is a type of malware that restricts users from accessing their important files / folders. This type of malware, forces its victims to pay the ransom through certain online payment methods in order to grant access to their files. **No antivirus or other security software can recover the data encrypted by ransomware**. Cryptolocker, Simplocker and CBT Locker are few examples of ransomware. The malware are targeting Windows PCs and Android devices..

2. **Method of Infection**. Ransomware can infect the system using various methods. Some of them are given below:-

a. Links received in emails.

b. Payload embedded in legitimate document or software received

c. through emails or USBs.

d. Files downloaded form Torrent sites.

e. Fake or free softwares.

3. **Capabilities of Malware**

a. Encrypts all documents and files.
b Encrypts drives and folders.
c. Shows a warning screen where user is asked to pay ransom within specific time. If the payment is not carried out, all files will be lost permanently.

4. **Recommendations.** In order to prevent from ransomeware, following is suggested:-

a. Backup your files regularly.

b. Download email attachments from trusted sources only. Even if a know contact sends a file, open it after confirmation.

c. Scan system regularly with antivirus.

d. Apply software patches regularly as some ransomware exploit vulnerabilities.

e. Install well reputed firewall with built-in HIPS (Host Intrusion Prevention System)