Advisory on Ransomware

What is Ransomware?

Ransomware is a type of malicious software designed to harm the computer system in its use. Ransomware infections such as Cryptowall, TeslaCrypt and Locky are a growing problem that is now affecting many computer users around the world. A further developed variant is Cryptolocker, which involves the encryption of important files and drives of the victim.

How Ransomware affects?

Files on computers and network drives gets encrypted as part of these infections, in order to blackmail the users of these computers and to pay a sum of money for the decryption tool.
Infection enters to Network through malicious Emails, Internet and using vulnerabilities within browsers.

These kind of threats keep changing their nature and it is required to be aware and vigilant always. Eg:. Threat would not infect initially when executed by user, it will just change the boot record and keep popping up a window for user to reboot. Once the system reboots, it does not enter the normal mode, instead boots in Safe mode and encrypts the machine.

Tips for Dealing with the Ransomware Threat, as and when detected:- Isolate the system from your network to prevent the threat from further spreading. Please perform below action urgently:-

- Remove the PC from Network.
- Don't share file from this System to other system.
- Don't use pen drive, external drives on this System to copy files to other systems.
- Get machine formatted completely and get fresh OS copy installed

Preventive Measures: To protect our computer against similar infections, user is to ensure the below mentioned preventive measures

- *Use and keep updated anti-virus software*

- *Blocking of removable media devices* - Prevent the use of all removable media devices on systems to limit the spread or introduction of malicious software and possible ex-filtration of data, except where there is a valid need for use.

- *Avoid opening suspicious emails* – To avoid clicking on suspicious links or opening suspicious attachments.

- *Not to use unsupported Operating system and applications* – Windows XP, Windows 2003, Internet explorer 6 or below and other applications which are currently not supported by vendors (end of life / end of support) are not to be used.

- *Restricting account privileges:-*. Configure all standard user accounts to prevent the execution and installation of any unknown or unauthorized software. Both standard and administrative accounts should have access only when required.