CYBER POLICE STATION
KOLKATA POLICE

ADVISORY ON WANNACRY RANSOMWARE

1. **What is Ransomware?**
   Ransomware is a malicious software that encrypts the contents of the Computer System and device and demands a ransom (money/bitcoin) to unlock it.
2. **What is WannaCry/WannaCrypt Ransomware?**
   A dangerous ransomware named 'Wannacry'/'WannaCrypt' encrypts the files on infected Windows System.
   All versions of windows before Windows 10 are vulnerable to this attack if not patched for MS-17-010. After a system is affected, it encrypts the files and shows a pop up with a countdown and instructions on how to pay the $300 in bitcoins to decrypt and get back the original files.
3. **How it is spreading?**
   It is spreading through malicious e-mail attachment. The ransomware spreads by clicking on links and downloading malicious files over internet and email. It is also capable of automatically spreading itself in a network by means of a vulnerability in Windows SMB. Initial ransom was of $300 but the group is increasing the demands upto $600 in bitcoin.

Do's	Don'ts
Ensure all Computers, Workstations and Servers have the latest Microsoft patches, especially the ones related to MS17-010.	Don't open attachment in unsolicited e-mails even if they come from the people in your contact list and never click on a URL content in an unsolicited e-mail.
Ensure AV (Anti-Virus) signatures are updated on all assets.	Don't open/click any pop-up on your web browser.
Apply Patch for vulnerabilities used by this ransomware from Microsoft and apply security updates from Microsoft, especially for MS17-010.	Don't enable auto-download option of your browser.
Block ports 139, 445 and 3389 in firewall.	Don't open file namely Mssecvc.exe and Taskche.exe.
Take regular back up of your important data and store offline.	Don't use crack Operating System and software on your computer.
Ensure that security solutions are switched on all nodes of the network.	Don't pay ransom.
Always keep installed security software up-to-date with latest signature updates.	Don't open any spam or unwanted e-mail.
Perform Full System Scan using installed security software.	

Note: If the system is infected by WannaCry/WannaCrypt Ransomeware:

- Immediately isolate the system from network.
- Preserve the data even it is encrypted.
- Report incident to concern law enforcement agencies.

****