# Dept. of IT & eGOV Advisory on Ransomware

## A. What is a ransomware attack?

Attacks involve malware delivered through spear phishing emails that lock up valuable data assets and demand a ransom to release them.
Hackers now check a victim's social media accounts, and create a fake email address pretending to be a friend or contact in order to get them to click on an infected link or attachment."It's much more targeted, and will exploit a particular vulnerability in a device, application, server or software, The Health / Education / social sector is highly targeted by hacker attacks, due to antiquated or misconfigured computer security systems and the amount of sensitive data they hold.

## B. How to Prevent Ransomware Attacks ?

1. Do not click hyper links from un-known sources, and without establishing authenticity of link even from known sources.
2. Prepare a up-to-date inventory of all the "Digital Assets" at various locations/facilities being used by the various functionaries of the organization.
3. Make a trustworthy knowledgeable functionary (permanent Government employee) Administrator of the Digital Assets (ADA) of the organization at each location.
4. Let ADA keep all software (especially the system software) up to date, including operating systems and applications.
5. ADA has to ensure back-up of all digital content located in the digital assets under ADA jurisdiction every day, including information on employee devices, so ADA can restore encrypted data if attacked by ransomware.
6. Back up all digital content to a secure, offsite secret location(s) within organization.
7. Distribute Back-up : Divide the digital assets and distribute the back-up locations. Don't place all data on one back-up file and share it.
8. ADA in collaboration with respective departmental officials, to train all the staff using the digital assets including mobile devices connected to network, on cyber security practices, emphasizing not opening attachments or links from unknown sources.
9. Develop a communication channel and strategy to quickly inform all employees if a virus reaches the company network.
10. If every bit of data of the organization is safeguarded and back-up is kept secretly, even if hackers attack and demand ransom, Govt can launch an investigation rather than making payment.
11. Mandate security auditing by ICERT empanelled auditors for all the digital assets as per GoI policy.
12. ADAs in collaboration with information security teams of ITE&C Dept and NIC to perform penetration testing to detect the vulnerabilities.
13. Register all the devices and digital assets. Strictly avoid usage of un-registered and unmonitored devices.
14. Adopt and use standard security and data privacy policies as per advisories from ITE&C Dept, NIC/ Govt of India.
15. Ensure all devices and systems are protected well with latest firewalls and anti-virus systems.

## C. Mitigating an attack

1. Remove the infected machines from the network, so the ransomware does not use the machine to spread throughout your network.
2. Report the attack and register all information related to attack.
3. Facilitate investigation of the attack.
4. Let one authorized spokesperson of the entire department only communicate with media the information related to attack.
5. A inventory of attacks and decryption kits / mitigation kits to be maintained