FACT SHEET – RANSOMWARE

What is Ransomware

Ransomware is a form of malware in which malicious software code holds a user's computer hostage until a "ransom" fee is paid to remove the restriction. Once installed, it makes the files unreadable on the hard drive. Infected users are then given a time limit to pay and after the elapsed period, the files become unrecoverable.

Types of Ransomware

With the recent technological development in the field of mobile devices, applications, social networks, and interconnected gadgets, there has been a sharp increase in ransomware attacks of different types. Some of the types of Ransomware are:

- **SMS Ransomware:** It locks the computer and displays a ransom message with a code. To unlock the computer, a code needs to be sent via text message to a premium-rate SMS number to receive the corresponding unlock code. In such cases, the ransom paid would be the cost of the premium rate text message.

- **Winlocker:** This one also locks the computer, but it displays a more intimidating ransom message, which appears to be from a law enforcement agency, indicating that the user has supposedly committed a cybercrime.

- **File Encryptors:** File Encryptors can encrypt files and folders using complex techniques to make the computer's data unusable. The Malware author then demands a payment against the decryption key using online payment systems.

- **Master Boot Record (MBR) Ransomware:** When this malware strikes, the ransom message is displayed as soon as the computer is switched on before loading the operating system itself.

Even if you make the payment, there is no guarantee that your computer's functionality or its data will be restored.

Sources of Ransomware

There are various ways to get infected:

- ✕ Clicking on an infected e-mail attachment
- ✕ Downloading an infected file from the Internet
- ✕ Sharing data or files on untrusted networks
- ✕ Visiting malicious or compromised websites
- ✕ Clicking on a malicious advertisement/link

Safeguards against Ransomware

- ✓ Always perform regular **backup**
- ✓ In suspicious cases, **disconnect** from the network
- ✓ Use only **official** software
- ✓ Share data or files only on **trusted** networks
- ✓ Secure your devices with an **updated** anti-virus software
- ✓ Avoid opening or downloading attachments from **unknown** sources
- ✓ Avoid clicking links on **suspicious** websites

In case you have fallen victim to Ransomware, please contact the relevant institutions.

Security Experts estimate that ransomware is cheating people out of more than Rs 120 M annually.

2.9% of users targeted by ransomware pay the cybercriminals.

Users may encounter ransomware via spam or malicious links. Once installed, it limits access to the system and displays a message requesting users to pay a ransom.

Ransomware is actually the second most popular type of malware being installed by cybercriminals.

To fool users, cybercriminals may use logos from Law Enforcement Agencies such as the Police, FBI or the CIA.

One of the Safeguards against Ransomware is to perform regular backup.