Title:

Unlocking the dangers of Ransomware with innovative defences

Dear Valued Customers,

Ransomware attack is a cyberattack where hackers encrypt victim's data and demand payment to decrypt it. It spreads through infected links or attachments, locking users out of their systems until they pay a ransom, typically in cryptocurrency.

These attacks cause financial losses, disrupt operations, and compromise sensitive information, posing a serious threat to businesses, governments, and individuals worldwide.

Modus Operandi:

- Threat actors send emails with malicious links or attachments disguised as legitimate files (e.g., PDFs, Office documents). They also use malicious advertisements on legitimate websites which redirect victims to websites hosting ransomware.

- Once executed on a system, ransomware starts encrypting files using strong encryption algorithms. Encrypted files become inaccessible to the victim, who receives a ransom note demanding payment in cryptocurrency (e.g., Bitcoin) to decrypt files.

- Fraudsters further instruct to pay the ransom and often threaten to delete files or sell it on dark-web.

- Paying the ransom does not guarantee file recovery or removal of malware, and this encourage further attacks.

Precautions:

- Ensure regular back up of important files to an external hard drives, or cloud storage service.

- Regularly update operating system, antivirus software, and applications from legitimate websites to protect against vulnerabilities.

- Avoid opening attachments or clicking on links in emails from unknown or dubious senders.

- Install licensed and effective antivirus software and keep it up to date to detect and block ransomware and other malware threats.

- Learn to recognize phishing attempts, where attackers attempt to trick you for revealing sensitive information or installing malware.

- Install software and files from trusted sources only. Verify the authenticity of websites before downloading anything.

For more information on cyber security awareness, refer BOI CYBER STAR E-Manual or Visit Safe Banking Section of our Website
Report cyber fraud under our Grievance section of our website and Also, on Govt. of India portal: www.cybercrime.gov.in OR CALL: 1930