Prevention Against Ransomware (Malware)

The information regarding Ransomware is published for the internet users of Punjab University under the direction of National Telecom and Information Technology Security Board (NTISB) for prevention against Ransomware.

Introduction:

Ransomware is a type of malware that restricts users from accessing their important files / folders. This type of malware, forces its victims to pay the ransom through certain online payment methods in order to grant access to their files. No antivirus or other security software can recover the data encrypted by ransomware. Cryptolocker, Simplocker and CBT Locker are few examples of ransomware. The malware are targeting Windows PCs and Android devices.

Method of Infection:

Ransomware can infect the system using various methods. Some of them are given below:-

- Links received in emails.
- Payload embedded in legitimate document or software received through emails or USBs.
- Files downloaded from Torrent sites.
- Fake or free softwares

Capabilities of Malware:

- Encrypts all documents and files.
- Encrypts drives and folders.
- Shows a warning screen where user is asked to pay ransom within specific time. If the payment is not carried out, all files will be lost permanently.

Recomendations:

In order to prevent from ransomware, following is suggested:-

- Backup your files regularly.
- Download email attachments from trusted sources only. Even if a known contact sends a file open it after confirmation.
- Scan system regularly with antivirus.
- Apply software patches regularly as some ransomware exploit vulnerabilities.
- Install well reputed firewall with built-in HIPS (Host Intrusion Prevention System)

Reporting of Suspicious Files / Emails:

Any malicious email / file may be reported to this organization on the following email address for analysis and suggesting mitigation measures:-

- eagle 1978@mail.com
- falcon098@writeme.com