Things to be done to protect the PC against Ransomware

Ransomware is malicious software that cyber criminals use to get hold of your computer files by encrypting data for ransom. It is designed to block system files and demand payment to provide the victim the key that can decrypt the blocked files. Ransomware is becoming an increasingly popular way for malware authors to extort money from companies and consumers alike. The following things can be done to protect your computer from ransomware.

1. First and foremost, be sure to **back up** your most important files on a regular basis.

2. Keep your **operating system**, **antivirus**, browsers, Adobe Flash Player, Java, and other software up-to-date.

3. Never **open or click** on attachment/ link from spam emails or suspicious emails or pop-up windows.

4. In the event a suspicious process is spotted on your computer, instantly turn off the Internet connection **by plugging out the internet cable** attached to your PC.

5. Switch off unused wireless connections, such as Bluetooth or Wi Fi spots.

6. Set unique passwords for different accounts to reduce the potential risk.

7. One way that Cryptolocker frequently arrives in a file that is named with the extension of **".PDF.EXE** or **TASKSCHE.EXE",** counting on Windows' default behaviour of hiding known file-extensions. You can check full file-extension by seeing properties by right clicking on the file and can easily spot suspicious files.

8. The Cryptolocker/Filecoder malware may access target machines using Remote Desktop Protocol (RDP), a Windows utility that allows others to access your desktop remotely. **One should disable RDP to protect your machine from RDP exploits. {Path = Control panel → System & Security → System → Remote setting → Don't allow connections to this computer}**