Users have to beware of Ransomware which can prohibit Windows users accessing their photos, personal documents, zip files and host of other files.

If you dare to update your system to Windows 10 based on fake emails from Microsoft, then you could be a victim of Cryptolocker Ransomware. The eScan research team has found that cyber-criminals are using various social engineering techniques to take advantage of millions of people looking for a free system upgrade to Windows 10 which was officially launched on July 29 worldwide .

What is Cryptolocker?

It is a kind of **Ransomware (/topic/ransomware)** which can prohibit Windows users accessing their photos, personal documents, zip files and host of other files. It makes use of asymmetric encryption i.e. Victims cannot access their files unless they have a private key, which is owned by the malware author and in order to obtain the key, the victim has to pay ransom amount to the cyber-criminal in virtual currency.

How does it work?

The malware enters into the user's system through a fake email from Microsoft even though cyber-criminal makes use of well-crafted email address update@microsoft.com making it appear as a valid one along with a subject line 'Windows 10 Free Update' and an attachment. The attachment was downloaded and executed by the research team and found a warning message along with instruction to pay $600 for the private key within 96 hours. The malicious email was traced to spam servers located in countries such as India, Russia, Thailand, USA and France.

What you need to do?

1. Users can update their current system to Windows 10 in two stages i.e. Reserve and Upgrade. In the first stage, users need to check whether they have got a notification in their taskbar from Windows which will reserve a free copy of Windows 10. On clicking the menu present on top left, it will check your system and run Windows Advisor to make sure that your hardware and software is compatible with Windows 10. Windows 10 will be downloaded once it is available. And the last stage is Installation where users will get a notification that Windows 10 is downloaded which needs to be installed.

2. Update your antivirus software on regular basis, which will protect your system from all kinds of Malware attacks.

3. Configure your antivirus settings to automatic system updates.

4. Regular backup of your important files.

5. Make sure you either implement Mailscan at gateway level or enable Mail Anti-virus on endpoint in order to block extensions such as *.EXE, *.SCR, *.JS, *.VBE etc. These attachments would infect your system.

6. Open emails only if you are positive about the source.