Cyber Security

Ransomware Remediation Process

Microsoft Removal Procedure -
http://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx

How to remove the ransomware depends on what type it is.

If your web browser is locked

You can try to unlock your browser by using Task Manager to stop the web browser's process:

1. Open Task Manager. There are a number of ways you can do this:
   - **Right-click** on an empty space on the taskbar and click **Task Manager** or **Start Task Manager**.
   - Press **Ctrl+Shift+Esc**.
   - Press **Ctrl+Alt+Delete**.
2. In the list of **Applications** or **Processes**, click on the name of your web browser.
3. Click **End task**. If you are asked if you want to wait for the program to respond, click **Close the program**.

When you open your web browser again, you may be asked to restore your session. Do not restore your session or you may end up loading the ransomware again.

If your PC is locked

- **Method 1: Use the Microsoft Safety Scanner in safe mode**

  First, download a copy of the Microsoft Safety Scanner from a clean, non-infected PC. Copy the downloaded file to a blank USB drive or CD, and then insert it into the infected PC.

  Try to restart your PC in safe mode:

  - In Windows 8.1
  - In Windows 7
  - In Windows Vista

  When you're in safe mode, try to run the Microsoft Safety Scanner.

- **Method 2: Use Windows Defender Offline**

  Because ransomware can lock you out of your PC, you might not be able to download or run the Microsoft Safety Scanner. If that happens, you will need to use the free tool Windows Defender Offline:

  - Download Windows Defender Offline

  Other Resources:

  Sophos - https://nakedsecurity.sophos.com/2013/10/18/cryptolocker-ransomware-see-how-it-works-learn-about-prevention-cleanup-and-recovery/

  PC World Article - http://www.pcworld.com/article/2084002/how-to-rescue-your-pc-from-ransomware.html

  TrendMicro Ransomware Removal Tool - http://esupport.trendmicro.com/en-us/home/pages/technical-support/1096206.aspx