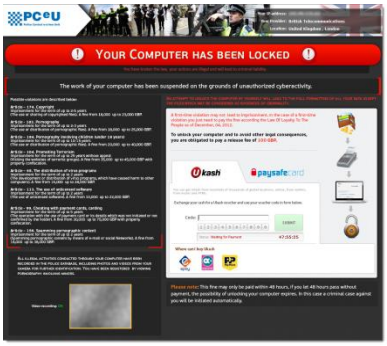
What is Ransomware?

Ransomware is malicious software that denies you access to your computer or files until you pay a ransom. There are two types of ransomware that are commonly seen:

- Encrypts personal files/folders (e.g., the contents of your My Documents folder - documents, spreadsheets, pictures, videos). Files are deleted once they are encrypted and generally there is a text file in the same folder as the now-inaccessible files with instructions for payment. You may see a lock screen but not all variants show one. Instead you may only notice a problem when you attempt to open your files. This type is called 'file encryptor' ransomware. For example, CryptoLocker is a file encryptor that most Anti-Virus programs detect as Troj/Ransom-ACP.

- 'Locks' the screen (presents a full screen image that blocks all other windows) and demands payment. No personal files are encrypted. Example screenshots of with type running on a computer are shown below. This type is called 'WinLocker' ransomware.



There is also 'MBR ransomware'. The Master Boot Record (MBR) is a section of the computer's hard drive that allows the operating system to boot up. MBR ransomware changes the computer's MBR so the normal boot process is interrupted and a ransom demand is displayed on screen instead.

What you can do to help avoid getting this infection:

- avoid opening any attachment emailed to you that you were not expecting.
- watch out for emails with attachments suggesting you must reply quickly or 'act fast' and hence feel compelled to open the attachment quickly - without considering the source.

Below are more screen shots of fake virus detection and/or ransomware lock screens. If you see any of the screens above or below on your computer, don't click on anything, call our office at (360)807-0266 immediately.