Ransomware - what is it, protection and removal

What is ransomware? Malicious software that locks a device, such as a computer, tablet or smartphone and then demands a ransom to unlock it.

Where did ransomware originate? The first documented case appeared in 2005 in the United States, but quickly spread around the world.

How does it affect a computer? The software is normally contained within an attachment to an email that masquerades as something innocent.

Once opened it encrypts the hard drive, making it impossible to access or retrieve anything stored on there – such as photographs, documents or music.

How can you protect yourself? Anti-virus software can protect your machine, although cybercriminals are constantly working on new ways to override such protection.

How much are victims expected to pay? The ransom demanded varies. There is no guarantee that paying will get your data back.

Read about the latest ransomware (WannaCry) at http://bbc.in/2r3fdpw. The ransomware encrypts your data and locks it until you pay a 'ransom'. It has become the largest ransomware attack in history, within a few hours. There is no guarantee, even if you pay the ransom, you will get your data back. It is recommended you do not pay the ransom.

The ransomware hits older Microsoft operating systems and those that have not been updated with a March patch from Microsoft.

According to Intel malware watch at http://bit.ly/2r2ATCi, the ransomware has gone worldwide and has hit NZ.

Take these seven steps ASAP to protect yourself:

1. Update all your software, especially any Microsoft Windows programs. Microsoft has made emergency updates available for Windows XP and 8, Vista, and other programs it had previously stopped supporting. The update is at http://bit.ly/2pOWrOY. Windows 10 is OK, providing it is up to date.

2. Backup your files. If you have an alternate or external backup drive

disconnect it meanwhile. It can also become infected. Take advantage of the free cloud backup services such as Dropbox, OneDrive, Google Drive, Mega and iCloud, among many others. These are easy to use, and can save you a lot of angst if you get hit with a ransomware attack. Back up all work and personal files to the cloud. You have access to them from any place or device.

3. Don't open attachments or click on links that seem even the slightest bit fishy or unusual.

4. Install the free CryptoPrevent programme from http://bit.ly/2r2Cisy, designed to identify and block ransomware.

5. Run the latest version of SUPERAntiSpyWare http://bit.ly/2pQaQdw, or Malwarebytes http://bit.ly/2pQ4PgV, free editions. Also

6. Try these removal tools

   - Trendmicro's Ransomware Removal Tool at http://bit.ly/2pS2t17 - a ransomware targeting removal tool available for Windows-based PCs.
   - Kaspersky's Ransomware Decryptor Site at http://bit.ly/2pRWwRO, is able to decrypt some types of ransomware.
   - View the tools at https://www.nomoreransom.org/, an initiative by the National High Tech Crime Unit of the Netherlands' police.

7. Use 'EMAIL Rule' to confirm that an email is dangerous. EMAIL means "examine message and inspect links."

   Check the 'From' line to show the email's sender.

   See if the subject line, is trying to create fear (e.g. "Your Account Will Be Closed") or entice you through curiosity (any subject line about payments, gifts or invoices) that grabs your attention.

   Look for spelling, grammar, or awkward wordings.

   Hover your mouse over every link in the email to see its real destination.

   If in doubt, the safest thing is to just delete any suspicious email. Anyone with serious business to conduct with you will persist to get in touch via social, phone, or snail mail.

For a copy of this article, with active links, email Alan Royal at :a.royal@paradise.net.nz.