What to do when your computer gets kidnapped by ransomware

October 30 2013, by Steve Johnson

Thousands of consumers are getting a nasty shock when they turn on their computers these days.

They find their screen frozen with an alarming note from what appears to be a government agency claiming they've accessed child pornography or committed other crimes and demanding money to unlock their machines.

If they fail to pay, the note warns, the authorities will lock them up next.

"It's probably the No. 1, end-user cybercrime now," said Kevin Haley, director of security response at Mountain View, Calif.-based Symantec. "It's pretty serious."

Experts say the risk of getting infected with "ransomware" can be minimized by making sure all of your software - including your antivirus programs - are updated regularly, not opening spam or email attachments from people you don't know and avoiding suspicious-looking websites.

If that doesn't work, you may have to wipe the computer completely clean and reinstall your files afterward. That assumes you have previously "backed up" or stored those files on a USB device, website service or some other way. If you haven't, your photos, financial records and other documents could be lost.

Windows-based computers often come with a recovery CD for restoring

the operating system and other pre-loaded software. But restoring files can be complicated, and people who aren't tech-savvy may need to get help from a computer-repair store or other experts.

"It's a nasty type of malware," concluded Andreas Baumhof, chief technology officer at San Jose, Calif., security company ThreatMetrix. "After one of these incidents, I'm sure people treat their online security differently."

Although the money-extorting scheme has been around for years, it gained notoriety in 2005, when Russian crooks began using it. Since then, it has evolved to become one of the world's most pervasive and aggravating cyber schemes.

Symantec, one of several companies offering a free ransomware removal service, recently reported seeing an "explosion of ransomware" spread by criminal gangs. In one case alone, it noted, 500,000 computers were infected over a period of just 18 days.

At least 16 variations of the scam have been documented. A typical version freezes the victim's computer with a message bearing an official-looking FBI logo, accusing the person of having visited child porn websites and of sending "messages with terrorist motives." It demands $200 or more to unlock the machine, adding, "you have 72 hours to pay the fine, otherwise you will be arrested."

In earlier versions, victims were told to pay the ransom by sending a premium-rate text message, which was charged to their phone bill. More recently, crooks have demanded payment via prepaid electronic systems such as MoneyPak. Those are sold for cash in stores and provide coded numbers used to pay bills online.

"A conservative estimate is that over $5 million a year is being extorted

from victims," Symantec's report said, though it added that the actual total is "likely much higher."

Experts generally advise against paying the ransom, because there's no guarantee the crooks will ever unfreeze the computer. If you do pay, said ThreatMetrix's Baumhof, all you can do is "hope and pray that the bad guys have some sense of humanity in them."

10 STEPS FOR REMOVING RANSOMWARE

Here's how to use a free Symantec service that the company says often removes the virus:

1. If the computer is Internet-connected, shut it off by holding down the power button for about 10 seconds.

2. Turn it back on while repeatedly tapping the F8 key.

3. When it brings up the "advanced boot options," use the down arrow to select "safe mode with networking" and hit "enter." You should see a screen that says "safe mode."

4. Open a browser - such as Google Chrome, Mozilla Firefox or Internet Explorer - and go to www.norton.com/npe

5. Click the button to download the Norton Power Eraser, save it to your desktop and double-click the icon to run the file.

6. After reading the user license and clicking "agree," click "scan for risks."

7. As Power Eraser restarts the computer, repeatedly hit the F8 button and again select safe mode with networking.

8. Click "run" so Power Eraser can scan for the virus.

9. Once it finishes, you'll see "scan complete" in a window with the results. Then click the "fix" button.

10. Click "restart" to reboot the computer again. You should see a confirmation that threat has been removed.