Spam and Spyware

It Takes Two: Senders and Receivers
By John Roy, President, The PC Users Group of CT
May 2012 issue, The Program
www.tpcug-ct.org
johnroy1 (at) comcast.net

As a recipient, everyone must be cautious before opening any email including those from family or friends. Fortunately, most ISPs do a fairly good job of stripping out obvious spam/malware email so it never reaches your inbox. You may even have a second filter to further reduce what arrives in your real mailbox but it is impossible to eliminate all spam/malware. Therefore, the final filter is a manual decision by you not to open a potential Spam/malware email.

Common sense about opening any questionable email has been published numerous times and need not be repeated here. Those of you that heed this generic advice will minimize your chances of becoming infected. The people that can't resist knowing what lies behind the questionable email will continually be infected. The bottom line is if it doesn't look right delete it. If you really think your friend sent something important, just respond requesting a follow up without opening the pending email.

Are you or your email address being flagged as the sender of this spam/malware? If you are being accused of sending spam/malware one or more of these things have happened.

- Your computer is infected and is sending this email without your knowledge.
- A friend of yours with your email address has a compromised computer that is sending the spam/malware using your email address.
- One or more of your email address passwords has been cracked and consequently compromised by a criminal.

Of course there could also be random spoofing of common email addresses. Some other clues that you may notice is getting replies or bounce messages to email you never sent.

So what can be done? When I receive a potential email threat from someone I know I first disable any active hyperlink and respond to the sender letting them know that spam/malware is being received from their email address. I recommend the person take preventative action by first running several malware tools such as Malwarebytes on their personal computer.

They can also change their ISP password in case that has been compromised. If the spam/malware source is someone else's computer or just random spoofing there really isn't much more that can be done but hope it eventually stops.