Re:News Article **Avoid Internet Doomsday: Check for DNSChanger Malware Now**

I've received many emails concerning this DNSChanger Malware. I have not had the infection and know little about it but I do have trusted sources who are experts in security matters. One of these is Mark Goldstein who came here a number of years ago when he was working with AOL and brought about changes in how we protect our computers from malware.

He took the information gathered here during the week they made house calls to people who were having problems with malware back to AOL and shortly thereafter AOL announced that they would furnish FREE McAfee Security to all it's customers. They were the leaders in furnishing FREE anti-virus programs to people using their email programs.

Mark is no longer with AOL. He now works totally with large scale security issues with large companies and government. Here is his take on this DNSChanger Malware issue.

Maxine –

I am very knowledgeable of this issue. DNSChanger is a very dangerous piece of malware. If a bad guy can tell your computer to find the IP address for Citibank, Bank of America, etc., on their DNS server, you are in big trouble. They hijack your DNS query so that you go to a fake Citibank login page and you give the bad guys your password. If someone controls your DNS, you can be hijacked anywhere.

a) Only the people who have been affected by DNSChanger malware will need to take action. The number is big but it certainly it not everyone who uses the Internet. You would know you have DNSCharger if you tried to go to a website and saw the message about being affected.

b) The FBI, Australian Police, and other international police agencies are doing the only logical thing to do which is protect the affected people from giving away their passwords to bad guys.

c) If someone with DNSChanger tries to connect to any website, they will get a message telling them they have malware and need to get it fixed. They also provide links to get fixes.

d) The police agencies do not want to be in the Internet business so they will shut down these "notification servers" in a few months. For the people who have not taken action to remove the malware after the FBI DNS servers are shut, they will no longer have DNS service which is essential to use the Internet. I view this like car inspections. If you have an unsafe car, you will not pass inspection because you can hurt yourself and others. If your computer is unsafe, the same will happen.

I follow issues in Washington closely and I have seen no activity in Congress, the White House, or the regulatory agencies to put any controls on what we can say or do on the Internet with the exception of illegal activity. The govt. has been active in stopping activities like child pornography, computer crime, and copyright infringement. One could argue that the govt has too many powers from the Patriot Act (i.e., wiretapping) but that has been around for Democratic and Republican administrations.

Mark