
From: [REDACTED]
Sent: Wednesday, February 22, 2012 12:08 PM
To: Lerner Lois G
Subject: RE: Virus on Home PC

MAC makes a difference in terms of the version of the software - as most software vendors sell a mac version vs a windows version of its product. But I think a mac should still have a software product regularly virus scanning. But I can research the apple site and confirm that for you.

Password strength is important, but many viruses are geared specifically towards using your email contacts for things like spam, so it could really be either.

[REDACTED]
TE/GE BSP-OMS
[REDACTED] (Office)
[REDACTED] (Mobile)

From: Lerner Lois G
Sent: Wednesday, February 22, 2012 1:04 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE: Virus on Home PC

It's not a PC--it's a MAC--I'm told by others that makes a difference--although I am computer illiterate(-: What's your take on that? My husband thinks I was simply hacked because my password was too simple. I don't believe anything I have a home is a must for sending to my work computer, so I think we are OK there. Thanks

Lois G. Lerner
Director of Exempt Organizations

From: [REDACTED]
Sent: Wednesday, February 22, 2012 12:59 PM
To: Lerner Lois G
Cc: [REDACTED]
Subject: Virus on Home PC

Good morning Lois. I'm sorry to hear about your problem with your home computer. I checked with MITS to get a couple of questions answered, as I wanted to give you as complete an answer as possible, to help with your problem.

1a - the home pc - I would start by getting online to the website of the company you have your virus software with (Norton, McAfee, etc) and make sure you have the most current updates to that software downloaded/installed on your computer

1b - once you know you have current virus definitions for your software - I would let it do a complete scan of the home pc - and hopefully it will find/quarantine any viruses present

2 - work data - if there is work data on the home pc that must be transferred back to your work laptop - MITS has a process by which that data and the electronic media carrying that data can be scanned in advance of accessing our network (I've included those steps below)

Any questions, please let me know.

██████████
TE/GE BSP-OMS

██████████ (Office)

██████████ (Mobile)

All forms of media received from U.S. taxpayers and other domestic IRS Business Partners shall be scanned for viruses/malicious code.

To configure your workstation to scan portable media (CD-ROMs, flash drives, floppy disks, etc.) you receive from taxpayers or IRS domestic business partners, follow these steps:

1. With your system connected to the network, ensure that the workstation is up to date with the MITS approved virus scanning software and signature.
 1. Right click on the gold shield at the bottom right hand corner of your computer screen. Open Symantec Antivirus.
 2. On the right side is a section titled "Virus Definitions File". In this section, there is a "Version". If the version is today's date, the computer is up to date. If the version date is not today's date, then run the Live Update by selecting the "LiveUpdate" button in this section.
2. Disconnect all network cables prior to accessing the media.
3. Insert the media and scan the media for viruses through the following steps:
 1. Access Windows Explorer by right clicking the start button at the bottom left of the computer screen.
 2. Select Explore with a left mouse click.
 3. Left mouse click the media drive.
 4. Right click Scan for Virus.
4. If the device is free of viruses, re-connect the network cables and proceed.
5. If a virus is detected:
 1. Do not re-connect the network cable.
 2. Do not power down or reboot the system.

3. Immediately contact CSIRC a [REDACTED] and your Frontline Manager, in accordance the Computer Security Incident Reporting Procedures, http://www.csirc.web.irs.gov/reporting/Incident_Reporting_Procedures.pdf

If you prefer not to perform the scan yourself, you can re quest a scan by contacting the Enterprise Service Desk [REDACTED].