Information System Security
Virus Detection Guidelines

A Mandatory Reference for ADS Chapter 545

New Reference: 06/01/2006
Responsible Office: M/DCIO
File Name: 545mbf_060106_cd44

Information System Security
Virus Detection Guidelines
for Users, HelpDesk and System Administrators

Computer virus – the term has come to mean any program, application, macro or other executable code that may damage or destroy the software or the data contained on computers. Viruses were originally small sets of code, written directly for the processor, to replicate or spread from computer to computer (normally by shared infected media or shared infected files spread through bulletin board systems and the Internet). Later, viruses included malicious code, specifically designed to do damage to the programs or destroy data. Virus writers then began to specialize, developing worms and Trojan horses. Worms spread without user action (normally by e-mail), and copy themselves from computer to computer across networks and the Internet. Trojan horses appear to be actual applications, but while they are executing, a virus or other malicious code is delivered to the computer. This malicious code is called a "payload."

Virus infections of all these types consume resources. Within a computer, a virus may use up all available disk space, wipe the computer hard drives, or monopolize the operating system (to send mail or perform other activity). On a network, viruses may consume all available bandwidth while replicating – this may include seeking out all hosts on the local area network or using the network to get to the Internet. No matter what the payload is or how the virus replicates, your computer will behave strangely.

While USAID has implemented anti-virus protection for the desktops, some servers, and e-mail systems, viruses can still get past these security controls and infect your desktop. When virus writers release new viruses "in the wild," there is normally a lag before the vendors update the anti-virus signatures. During this lag, your computer is vulnerable.

You should always be on the lookout for unusual behavior that could indicate that your computer may be infected. In the list that follows, "disk drive" means hard disk drive, CD-ROM drive, or diskette drive. "Files" means both application (program) and data files. Some basic signs of a possible infection are:

- You cannot access the disk drive.
- You cannot access the network, or the network connection appears "slow" or "sluggish."
- You cannot print or your applications do not work properly.
- You notice unscheduled disk drive activity.
- You notice that your hard disk is full.

- You notice changes to stored files – new files, changes to file sizes, access dates, or content.
- You notice unusual error messages or dialog boxes.
- The system slows down, locks-up, or crashes unexpectedly or repeatedly.

Some technical signs of an infection are:

- You receive notification that you have sent e-mail that you did not send.
- You notice that the anti-virus program is disabled and you cannot restart it.
- Your e-mail sent folder has messages (that you did not send) to everyone in your e-mail list.
- You notice double extensions on your files, such as .txt.exe or .dat.vbs.
- You notice that there are unexpected files with the extensions .exe, .cmd, .bat, .vbs, .scr.
- You notice that the security settings for your computer or your browser have been altered to lower their level or to permit remote access.

Specific to the USAID environment:

- You notice that Windows will not start or indicates that critical system files are missing.
- You notice that Windows starts, but locks up before the desktop or task bar appear.
- You receive out-of-memory errors or the system runs slowly or starts slowly.
- You cannot work with the Microsoft Office suite, start the programs, or reinstall them.
- You cannot start the Task Manager or system applications, or they report errors.
- The anti-virus software indicates an unknown virus is present, or a virus is present that the software cannot successfully “clean.”

If you know or suspect that your computer is infected with a virus, you must follow this procedure:

- Stop what you are doing.
- Save your work.
- Do not send e-mail to anyone, not even to inform the local Help Desk of the virus. Sending e-mail may spread the virus to other computers.
- Phone the local Help Desk immediately to report the virus.
- Provide the local Help Desk with as much information as possible about the symptoms you’ve experienced, and include any information from alert files or pop-up windows.

- If the anti-virus software has identified the virus, provide that information to the local Help Desk.
- If you have exchanged files with another user recently, via e-mail attachment, CD-ROM, or diskette, inform the local Help Desk. The files may be infected and need to be cleaned.
- If you have stored any files off-line or on a network drive, inform the local Help Desk. The files may be infected and need to be cleaned.
- Follow any local Help Desk instructions.

Generally, the Help Desk will use an anti-virus program to identify the infection; the Help Desk will look up the virus in a catalog and determine the necessary course of action. If the virus cannot be identified or the infection is severe, then the Help Desk may need to rebuild your machine. Once the virus has been successfully cleaned, then you may resume normal work activities.

In the event you cannot contact or do not have a local or regional helpdesk you may contact the IRM Help Desk in Washington, DC at 202-712-1234.