7.1.3 Malware Protection Facts

Regardless of the type of malware, there are some common things you can do to prevent malware infection:

- Use the latest version and patch level for your web browser
- Install the latest patches for the operating system
- Install antivirus, anti-spyware, anti-rootkit, and personal firewall software
- Keep definition files up-to-date
- Use a pop-up blocker to prevent adware
- Use software to control cookies on the system
- Perform regular scheduled scans to look for malware
- Choose anti-malware software from a reputable company (don't let scareware fool you into purchasing a product that may not work)

In addition, implement the following measures:

- Train users not to download files from unknown sources or open files in suspicious emails. Spyware, adware, crimeware and Trojans all take advantage of downloads
- Remove removable drives to prevent unauthorized software entering a system.
- Show full file extensions on all files. Viruses, worms, and Trojans often make use of double file extensions to change the qualities of files that are normally deemed harmless. For example, adding the extension .TXT.EXE to a file will make the file appear as a text file in an attachment when, in reality, it is an executable.
- Enable antivirus scanning for all email attachments.
- Enable antivirus scanning for all removable storage, such as USB flash drives and CD-ROMs.
- Block executable files that have been copied from another computer and require that they be manually unblocked before execution.
- Enable privacy controls in Windows Internet Explorer to:
  - Delete browsing history
  - Configure Autocomplete settings not to store entries such as usernames, passwords, web addresses, and forms
- Use third-party tools to scan for issues and cleanup problems.

Recovery from malware could include the following steps:

- Malware can permanently damage your system. You may have to reinstall applications, features, or even the entire operating system from scratch.
- If your organization uses imaging solutions, you can quickly re-image a machine if it is infected with malware. Re-imaging or installing from scratch is often faster and more effective than malware removal and cleanup.
- *Remediation* is the process of correcting problems. Most antivirus software remediates problems automatically or semi-automatically by prompting you to identify the action to take. Possible actions in response to problems are:
  - Repair the infection. Repair is possible for true viruses that have attached themselves to valid files. During the repair, the virus is removed and the file is placed back in its original state (if possible).
  - Quarantine the file. Quarantine moves the infected file to a secure folder where it cannot open or run normally. You might quarantine an infected file that cannot be repaired to see if another tool or utility might be able to recover the file at another time.
  - Delete the file. You should delete malicious files such as worms, Trojan horse programs, spyware, or adware programs. In addition, you should periodically review the quarantine folder and delete any files you do not want to recover.