

GENERAL SERVICES ADMINISTRATION
WASHINGTON, DC 20405

November 6, 1990

FIRMR BULLETIN C-28

TO: Heads of Federal agencies
SUBJECT: Computer viruses

1. Purpose. This bulletin provides guidance to Federal agencies regarding protecting Government computers from harm caused by destructive code routines commonly called computer viruses. It also provides guidance regarding the use of public domain software.

2. Expiration date. This bulletin will remain in effect until canceled or superseded.

3. Contents. This bulletin address the following topics:

Topic	Paragraph
Related material	4
Information and assistance	5
Definitions	6
Discussion	7
Common entry for viruses	8
Use of public domain software	9
Network security	10
Security planning	11

4. Related material.

National Institute of Standard and Technology special (NIST)
Publication 500-166.

5. Information and assistance.

a. Request for assistance or additional information on
computer viruses can be obtained from:

National Institute of Standard and Technology
Computer Security Resources and Response Center
A-216 Technology
Gaithersburg, MD 20899
Telephone: (301) 975-5200

TC 90-1

FIRMR Bulletin C-28

b. Request for assistance or information regarding this bulletin should be directed to:

General Services Administration
Regulations Analysis Division (KMR)
Washington, DC 20405
Telephone: (202) 501-3194 or FTS 241-3194 (v)
or (202) 501-0657 or FTS 241-0657 (tdd).

6. Definitions.

"Public domain software" means software known as freeware and shareware available to the public.

"Freeware" means software whose author allows others to use it without charge.

"Shareware" means software marketed by sharing it among users; if a prospective customer decides to keep the software, the customer remits a license fee.

"Viruses" means microcodes that would normally provide useful applications to the user. These microcodes enter a system without the user's consent or knowledge, and interfere with the system's normal operation. This interference may be merely to display a message but may also be to cause loss or alteration of data.

7. Discussion. Recent Government and industry experiences have shown that computers are vulnerable to alteration or destruction of data by the introduction of code routines commonly referred to as "computer viruses." These destructive code routines are spread by many methods, including use of the programs for a specified number of interactions or by a built-in time delay. A virus may initially infect only one computer in an organization, but the virus's parasitic traits may allow it to attach to other programs that are shared among computers throughout the organization. Since viruses can travel from one place to another as fast as a phone call or exchange of floppy diskettes, a single virus strain can quickly turn up in computers hundreds of miles apart. As a result, nationwide systems can be infected almost overnight.

8. Common entry for viruses. Protecting agency computers and the information used on them requires knowledge of the vulnerabilities of computer systems to viruses. Common points of entry for viruses include diskette swapping among users, downloading from infected bulletin boards, infected network servers, and in a few cases, shrink-wrapped software diskettes, as well as access of computer systems by unauthorized users.

FIRMR Bulletin C-28

9. Use of public domain software. The level of investment in equipment, time and records mandates that quality software be used. Public domain software does not always meet this criterion. It may also suffer from inadequate documentation, absence of training materials, maintenance and warranties. Due to these deficiencies and the added threat of contracting a virus, agencies should test public domain software with anti-viral software before permission to use is granted. Many types of virus infections can be prevented by adhering to the following security precautions:

- a. Ascertain how reputable a bulletin board is before using it. Test all downloaded software for viruses before it is used. Download software to a "stand-alone" computer where it can be evaluated prior to installation on a network.
- b. At random, use anti-viral software to assist in protecting the integrity of systems that process sensitive information.
- c. Restrict the use of public domain software programs. Avoid putting such software in the main directory (or common file server directory if on a network).
- d. Limit system access to authorized personnel who have been thoroughly briefed on virus prevention techniques.
- e. Keep original application disks in a secure location so they cannot be infected. Protect diskettes by using "write protect" stick on labels.
- f. Since viruses can infect hard disks when booted from a floppy disk, use only the original distribution floppy disk that is always write protected.
- g. If operating a system with only floppy drives, boot from only one, clearly labeled, previously tested, write-protected floppy disk.
- h. Rely predominantly on a trusted collection of commercial applications for software, if using a standalone system, as there have been very few cases of contaminated commercial software.
- i. Remove all public domain software from agency computers unless the software has been thoroughly tested by a system administrator or his equivalent, the bulletin board from which the software was downloaded, or another reliable source.

10. Network security. Network hardware and software companies offer security options and software that can help detect viruses. Another precaution involves use of a dedicated server set so that data can be downloaded but never uploaded. That way, a virus that spreads through individual workstations could never corrupt the data on the server or other systems accessing the server. Use anti-viral software on the servers regularly and do not create common directories of software unless the software is tested regularly for viruses. Provide maximum protection for the server, as infected software on a server could be disastrous. Other devices, such as computers and "bridges", can also perform the guard functions necessary to enforce multilevel security.

11. Security planning.

a. Each agency should develop a strategy to help prevent or limit the spread of a virus. A number of methods exist for doing this. Software programs have been developed which identify a specific strain of a virus and remove the virus from the infected disk. These programs will work only for a particular strain, however, and are not generally effective for other strains of viruses. Once a compromised program is cleaned, it still may not be usable due to damage caused by the virus. hardware solutions which offer protection against viruses are also available. Although there is no foolproof way to protect against a virus, certain actions such as limiting program sharing, performing frequent backups, controlling system access, and screening downloaded software, are good defenses.

b. A contingency procedure should be developed and distributed for containing a system virus that is suspected or identified.

c. NIST recently issued guidelines for controlling viruses in various computer environments including personal computers and networks. Computer Viruses and Related Threats: A Management Guide (NIST Special Publication 500-166), is available from the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402. Order by stock No. 003-003-02955-6 for \$2.50 prepaid.

Thomas J. Buckholtz
Commissioner
Information Resources
Management Service

