Computer Viruses (part 4 of 4)

This article last reviewed: 15 April 1988

SAFEGUARDING YOUR SYSTEMS

What Makes Our System Susceptible to Viruses

The various mechanisms described in part 2 of this article make our
system easy to infiltrate by a virus. Remember that it is those same
mechanisms that add to the flexibility and "look and feel" of the Macintosh.
For instance, the INIT mechanism is used by mail systems to load their code
in. AppleShare uses the INIT mechanism to mount network volumes at boot
time.

Why Vaccine Works in This Case, But Is Easy to Bypass

Vaccine, a public domain INIT written to block viruses, does a good job of
alerting you when the three known viruses are trying to infect your system.
The problem with Vaccine: once a cure is found for one set of viruses,
a new strain may appear that knows how to bypass the existing defenses.

Some Suggestions

- Lock your master diskettes

  Always keep original "Master" disks locked. This prevents a virus from
  spreading to your original disks. Our disk locking mechanism is hardware
  based -- viruses can't infect locked disks!

- Protect your networks

  Network administrators should not allow just anyone to put software on
  the server. Applications on a network server should come only from
  known good masters.

- Be wary of public domain software

  Public domain software should be checked quite thoroughly on a floppy-
  based system for any infections before being copied to a hard disk based
  system. This will also protect you from any "Trojan Horse" programs such
  as "Sexy Ladies."

- Quarantine infected systems

  If you identify a system as being infected with a virus, immediately
  isolate (quarantine) it from other systems. This means disconnecting it
  from any network and not allowing anyone to take any files from the
  exposed system to another system. Once the system has been 'disinfected,'
  you can allow the files to be copied or moved.

- Use ResEdit

  ResEdit is a good tool to look for viruses on your disks. There is very
  little that can be hidden from ResEdit, so you can use it to remove
  troublemaking files and resources.
Copyright 1989 Apple Computer, Inc.

Keywords: <None>

===

This information is from the Apple Technical Information Library.

19960215 11:05:19.00
Tech Info Library Article Number: 2824