Recommendations for Keeping Your System Virus-Free

This appendix provides recommendations to help you avoid virus infections on your system. Some of the recommendations are intended for all users, while others are more suited to people who manage Macintosh networks.

Recommendations for All Users

While there is no need to panic over viruses, they should be taken seriously. Using VirusScan, it only takes a few minutes per week to effectively protect your Macintosh against known viruses. The following recommendations may help you:

- If you do nothing else, consistently use the VirusScan extension. It only takes a minute to install and, by neutralizing viruses before they can damage your data, it can save you time, money, and aggravation.
- Keep original software on locked diskettes. Use copies. When you obtain a new piece of software, immediately lock the disk on which it came, make a copy, and use the copy. Never unlock the original disk. It is impossible for a virus to infect files on a locked floppy.
- Make periodic backups of your hard drive at least once a week.
- Make sure you are using the latest version of VirusScan. The current version of VirusScan only protects your system against viruses that were known at the time of its release. As new viruses are discovered, VIrusScan is updated to detect them.

In most situations, this is all you need to do to protect your Macintosh against viruses. You do not need to scan all new applications or new diskettes before using them. As long as you have the extension properly installed, it will detect and block viruses before they can spread or cause any damage.

The extension also makes it unnecessary to scan your hard drives frequently. However, you should do a full scan of your hard drives periodically just to make sure that they are still uninfected. For example, if you start up from a floppy disk that does not have the VirusScan extension installed, it is possible for a virus to infect your hard drives. For instance, you might want to do a full scan before every backup. This will also make sure that your backups are clean.

Recommendations for System Administrators

The following recommendations are for people who manage Macintosh networks, laboratories, bulletin boards, or collections of public domain and shareware software. An environment where many people share computers is a perfect breeding ground for viruses. People who sell software also have a special responsibility to make sure that their software is free from infection.

- Install the VirusScan extension on all your startup disks.
- Check all diskettes frequently with VirusScan to make sure they're uninfected. Also check to make sure that the VirusScan protection extension is still installed and active on all your startup disks.
- Educate the people in your organization about viruses and how to protect against them. Give them copies of VirusScan and teach them how to use the application. Distribute copies of this manual.
- Try to put software in write-protected folders on AppleShare server disks. Viruses cannot infect applications if they are in folders that do not have the "Make Changes" privilege. On the other hand, if an application is in a writable server folder, any infected Macintosh on the network that accesses the disk and uses the application might spread the infection to the application on the server. If it is a popular application, it will in turn quickly infect any other Macintoshes on the network that are not protected by a protection extension. This is one way in which viruses can spread very rapidly. Since some applications insist on writing to their own file or folder, it is not always possible to put applications in write-protected folders, but you should do this when possible.
- Check server disks frequently with VirusScan to make sure that they are uninfected. For best results, you should take the server out of production and restart it using your Virus Tools or Disk Tools disk. This is the only way to guarantee that VirusScan will be able to scan all the files on the server disk. For more information about creating a Virus Tools disk, see "Before you start" on page 18.
- Check all new software with VirusScan before installing it on a server.
- Back up you servers frequently. Run VirusScan just before each backup

- The WDEF virus can cause serious performance problems if it infects an AppleShare server. To avoid these problems, administrators should never grant the “Make Changes” privilege on server root directories. We also recommend deleting the Desktop file if it exists.

- Bulletin board operators and other people who maintain and distribute public domain and shareware software have a special responsibility to the Macintosh community. Please carefully test all new software before distributing it. Of course, you should also run VirusScan on all new software you receive.

- If you sell software, please check your master disks for infections before sending them out to be duplicated and distributed.