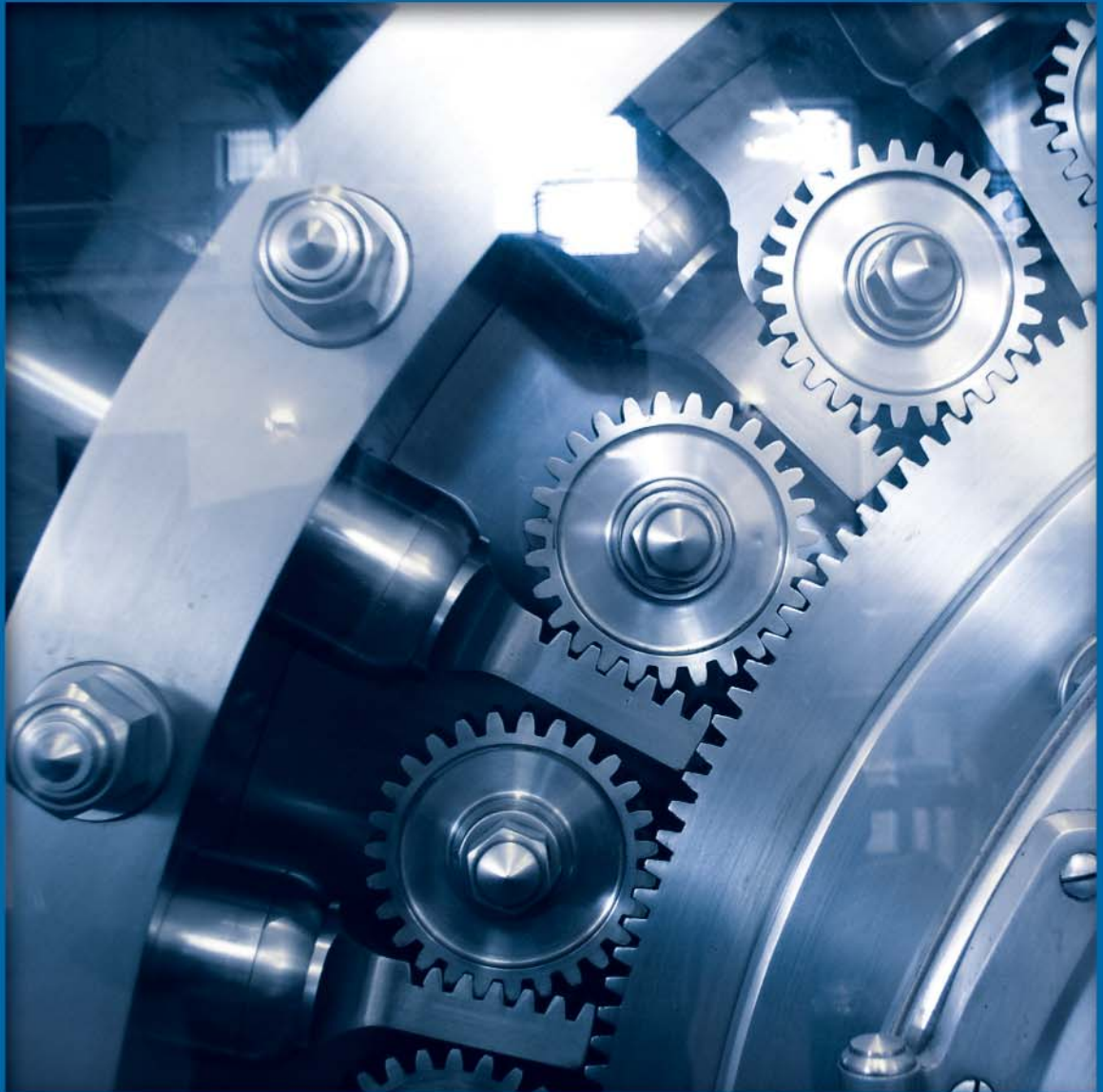


TechRepublic  
Real World Guide

---

# Virus Prevention and Recovery



TechRepublic Real World Guide:  
Virus Prevention and Recovery

**Director, TechRepublic Press**

Carmen Barrett

**Executive Editor,**

**Premium Products**

Erik Eckel

**Operations Manager**

Marilyn Bryan

**Graphic Artist**

Kimberly Wright

**Senior Editor**

John Sheesley

**Promotions Manager**

Megan Hancock

**Customer Service Manager**

Elisa Suiter

**Copyright ©1995-2005**

by CNET Networks, Inc. All rights reserved.  
TechRepublic and its logo are trademarks  
of CNET Networks, Inc. All other product  
names or services identified throughout  
this book are trademarks or registered  
trademarks of their respective companies.  
Reproduction of this publication in any form  
without prior written permission is forbidden.

**Disclaimer**

The information contained herein has  
been obtained from sources believed to  
be reliable. CNET Networks, Inc. disclaims  
all warranties as to the accuracy, complete-  
ness, or adequacy of such information.  
CNET Networks, Inc. shall have no liability  
for errors, omissions, or inadequacies in  
the information contained herein or for the  
interpretations thereof. The reader assumes  
sole responsibility for the selection of these  
materials to achieve its intended results.  
The opinions expressed herein are  
subject to change without notice.

**TechRepublic**

1630 Lyndon Farm Court

Louisville, KY 40223

Tel.: 1.800.217.4339

Online Customer Support:

<http://www.techrepublic.com/cshelp>

Published by TechRepublic

July 2005

**Table of Contents**

Antivirus policies should educate users and outline responsibilities.....3  
Sample Virus Protection Policy .....4  
Be ready to react when an e-mail virus strikes .....7  
E-mail virus attack checklist .....10  
Address antivirus software in your disaster recovery plan .....13  
Virus prevention Checklist .....15



# Antivirus policies should educate users and outline responsibilities

By Mike Walton

A crucial part of an antivirus strategy is having a written policy that defines both the IT department's and end user's roles in protecting your network. The policy should also provide users with a basic understanding of how viruses spread and how they can help prevent virus attacks. To help you create such policy for your organization, TechRepublic has produced a sample virus protection policy, which follows at the end of this article.

## Nothing is foolproof, but a policy can help designate the fool

You can't force people to read or heed a policy. One thing a policy can do, however, is put users on notice that they are also responsible for network security.

Granted, such a policy doesn't absolve the IT department from its duty to protect the network. But the IT department doesn't deserve all the blame when the same user opens an I LOVE YOU message for the 10th time.

Use our template as a starting point to develop a policy that fits your organization. Your procedures for dealing with virus attacks will depend greatly on the antivirus software you use and your organization's general philosophies on end-user responsibilities.

Some support pros advise users to call them before doing anything to a suspicious e-mail, even deleting it. And to test whether users are following that antivirus procedure, they send random, anonymous e-mails to them as tests!

## Educate, illustrate, and enlist

One of the most effective ways to enlist end-user support is to give them appropriate information and show them what the IT department is doing to help reduce their risk.

Enlisting the user's help has the advantage of involving the user in the organization's security at a basic level. Some IT pros may even be able to show users that changing their e-mail behavior at work may carry over into their personal computer usage at home and save them some grief.

## Sample Policy

To help you create a virus protection policy that fits your organization's needs, we've created the following sample policy. Use this sample as your guideline when creating or updating your company's virus protection policy. ❖

# Sample Virus Protection Policy

Date issued:

Revised:

Authorized by:

Next scheduled review:

Introduction

It is the responsibility of everyone who uses [organization]'s computer network to take reasonable measures to protect that network from virus infections.

This policy outlines how various viruses can infect [organization]'s network, how [organization]'s IT department tries to prevent and/or minimize infections, and how [organization]'s network users should respond to a virus if they suspect one has infected [organization]'s network.

## How viruses can infect [organization]'s network

There are actually three various types of computer viruses: true viruses, Trojan horses, and worms. True viruses actually hide themselves, often as macros, within other files, such as spreadsheets or Word documents. [Note: Viruses can actually hide themselves in a variety of mediums: applications, boot sectors, partition sectors, and so forth, but this information is most likely too complex for the average end user. It's better to only include the basics.] When an infected file is opened from a computer connected to [organization]'s network, the virus can spread throughout the network and may do damage.

A Trojan horse is an actual program file that, once executed, doesn't spread but can damage the computer on which the file was run. A worm is also a program file that, when executed, can both spread throughout a network and do damage to the computer from which it was run.

Viruses can enter [organization]'s network in a variety of ways:

- **E-mail**—By far, most viruses are sent as e-mail attachments. These attachments could be working documents or spreadsheets, or they could be merely viruses disguised as pictures, jokes, etc. These attachments may have been knowingly sent by someone wanting to infect [organization]'s network or by someone who does not know the attachment contains a virus. However, once some viruses are opened, they automatically e-mail themselves, and the sender may not know his or her computer is infected.
- **Disk, CD, Zip disk, or other media**—Viruses can also spread via various types of storage media. As with e-mail attachments, the virus could hide within a legitimate document or spreadsheet or simply be disguised as another type of file.
- **Software downloaded from the Internet**—Downloading software via the Internet can also be a source of infection. As with other types of transmissions, the virus could hide within a legitimate document, spreadsheet, or other type of file.

**True viruses actually hide themselves, often as macros, within other files, such as spreadsheets or Word documents.**

- **Instant messaging attachments**—Although less common than e-mail attachments, more viruses are taking advantage of instant messaging software. These attachments work the same as e-mail viruses, but they are transmitted via instant messaging software.

## How [organization]’s IT department prevents and/or minimizes virus infections

[Organization]’s IT department fights viruses in several ways:

- **Scanning Internet traffic**—All Internet traffic coming to and going from our network must pass through company servers and other network devices. Only specific types of network traffic are allowed beyond the organization’s exterior firewalls.

For example, an e-mail message that originates outside of the network must pass through the [your antivirus protection firewall] before it is allowed to enter the e-mail server. This device routes suspicious e-mail and attachments to an isolated storage device, defeating the purpose of a virus.

- **Running server and workstation antivirus software**—All vulnerable servers run [antivirus scanning software]. This software scans our file-sharing data stores, looking for suspicious code.

[Antivirus protection software] is also installed on all organization workstations. This software scans all data written to or read from a workstation’s hard drive. If it finds something suspicious, it isolates the dubious file on the computer and automatically notifies the help desk.

- **Routinely updating virus definitions**—Every morning, the firewall and server virus scanning programs check the [antivirus program’s control center] for updated virus definitions. These definition files allow the software to detect new viruses. If a new virus definition file is available, the virus scanning software is automatically updated, and then the system administrator is informed.

When end users turn on their computers at the beginning of the workday, the workstation virus protection program checks with a [organization] server on the network for updates. The workstation program will then download and install the update automatically, if one exists.

## How to respond to and report a virus

Even though all Internet traffic is scanned for viruses and all files on the company’s servers are scanned, the possibility still exists that a new or well-hidden virus could find its way to an employee’s workstation, and if not properly handled, it could infect [organization]’s network.

The IT staff will attempt to notify all users of credible virus threats via e-mail or telephone messages. Because this notification will automatically go to everyone in the organization, employees should not forward virus warning messages. On occasion, well-meaning people will distribute virus warnings that are actually virus hoaxes. These warnings are typically harmless; however, forwarding such messages unnecessarily increases network traffic.

As stated, it is the responsibility of all [organization] network users to take reasonable steps to prevent virus outbreaks. Use the guidelines below to do your part:

- Do not open unexpected e-mail attachments, even from coworkers.
- Never open an e-mail or instant messaging attachment from an unknown or suspicious source.
- Never download freeware or shareware from the Internet without express permission of the IT department.
- If a file you receive contains macros that you are unsure about, disable the macros.

### **Notify the help desk of suspicious files**

If you receive a suspicious file or e-mail attachment, do not open it. Call [organization]'s help desk at extension [extension number] and inform the support analyst that you have received a suspicious file. The support analyst will explain how to handle the file.

If the potentially infected file is on a disk that you have inserted into your computer, the antivirus software on your machine will ask you if you wish to scan the disk, format the disk, or eject the disk. Eject the disk and contact the help desk at extension [extension number]. They will instruct you on how to handle the disk.

After the support analyst has neutralized the file, send a note to the person who sent/gave you the file notifying them that they sent/gave you a virus. (If the file was sent via e-mail, the antivirus software running on our e-mail system will automatically send an e-mail message informing the sender of the virus it detected.)

If the file is an infected spreadsheet or document that is of critical importance to [organization], the IT department will attempt to scan and clean the file. The IT department, however, makes no guarantees as to whether an infected file can be totally cleaned and will not allow the infected file to be used on [organization] computers.

Your signature indicates that you have read [organization]'s virus protection policy. Your signature does not mean that you agree with each and every provision of the policy. However, it does indicate that you will abide by the regulations set forth in the above policy.

Employee:

Date:

---

---



# Be ready to react when an e-mail virus strikes

By John Sheesley

One of the most common ways for organizations to suffer a virus attack is via e-mail. Since the Melissa virus first raised the issue on a large scale in March 1999, e-mail viruses have grown in “popularity.” If one hasn’t struck your organization yet, it probably will soon. What you need is a strategy to react and minimize the disruption. To help you follow the appropriate steps for recovering from an e-mail virus infection, we’ve put together an e-mail virus attack checklist, which follows at the end of this article.

## Don’t panic

As soon as you notice something odd and virus-like going on in your e-mail system, it’s tempting to reach over and pull the network cable out of the e-mail server to prevent any virus from getting loose. Although that might be an emotionally satisfying reaction, it’s not one that best minimizes the impact of an e-mail virus attack.

The best way to deal with an e-mail virus outbreak is to take a measured, step-by-step approach. Some of the things you should do include the following:

- Identify the problem.
- Communicate with end users.
- Stop the virus.
- Clean up the mess.
- Perform a postmortem.
- Prepare for the next attack.

## Identify the problem

E-mail viruses can take three forms: viruses, worms, and Trojans. Knowing what kind of virus you’re dealing with will help you figure out the severity. Also, don’t forget that some virus warnings are actually hoaxes. Make sure that you’re dealing with an actual virus before you go into firefighting mode.

Once you know that you’re dealing with an actual virus, find out where it came from. If you can, find out who e-mailed it and who in the organization got the e-mail first. This will help you warn the people that your organization deals with that they may be facing an attack. You may also be able to find out how they handled the attack to get some clues to help solve the problem.

Remember that different e-mail systems are affected by different viruses. For example, a virus that reacts one way on Outlook/Exchange may not affect GroupWise and GroupWise clients. Do some research to learn how the virus you’re facing affects the e-mail system you’re using.

You should also know what virus scanner is running on both your e-mail server and your clients, in case you need emergency updates. Check with the virus protection

maker to see whether it has provided a patch for the virus you've been hit by and whether you need to obtain updates or patches.

## Communicate with end users

Let users know there's an e-mail virus attacking the network, but do so in a manner that doesn't cause panic. If need be, use instant messages or phone calls for notification. In a small organization, you may be able to deliver the warnings in person.

Find out who has been infected with the virus and who hasn't. It may help identify the source of the virus and how it's spreading in your organization.

## Stop the virus

If the virus is spreading fast, you may need to immediately disconnect your e-mail server from the network. Some viruses propagate from client workstation to client workstation. If many clients are affected, you may need to bring down the whole network. The fastest way to do so may be by just shutting down hubs, switches, and routers in your organization. Of course, you should warn users before doing this.

If you haven't recently obtained virus signature updates for the server, do so immediately using a machine that hasn't been infected. You may also need to download any special cleaning utilities the vendor has. After you have the utilities, apply and run them.

## Clean up the mess

Run the updated virus scanner or utilities you've downloaded against the mail server and any affected workstations. You may need to use a utility like IISScan or ExMerge from Microsoft to physically delete infected messages.

Some viruses also damage user mailboxes. Make sure you have backups handy to recover the mailboxes.

You may need to completely reinstall the operating system, applications, and e-mail clients on client workstations. Make sure you have backups handy for those as well.

## Perform a post-mortem

After you've dealt with the attack and have things back to normal, go over your notes. When you're not in the middle of the attack, you'll have more time to identify where the attack came from and to decide how to react in the future.

## Prepare for the next attack

Naturally, the best way to deal with an e-mail virus attack is to avoid facing it to begin with. Some ways to minimize your vulnerability in the future include:

- Ensuring that you have an e-mail virus scanner on your e-mail server as well as on your clients.
- Making sure that all virus signature updates are current.
- Educating users about opening attachments to e-mails.

---

**If the virus is spreading fast, you may need to immediately disconnect your e-mail server from the network.**

- Creating an alternate communication structure in your organization for when e-mail fails.
- Verifying that your backup routine functions properly and that backups remain current.

Because Outlook and Exchange are the most popular targets for e-mail virus attacks, some organizations have even gone as far as replacing them with Lotus Domino, Novell GroupWise, or a Linux-based e-mail system. Depending on the size of your organization, this may be a consideration for you as well. ❖

# E-mail virus attack checklist

Topic	Questions to ask	Description
<b>Identify the attack</b>		
<input type="checkbox"/> Virus, worm, or Trojan	What kind of virus are you facing?	E-mail viruses can take three forms. Knowing what kind of virus you're dealing with will help you better figure out the severity. Don't forget that some viruses are actually hoaxes.
<input type="checkbox"/> The carrier	Where did the virus come from?	Find out where the virus came from—who e-mailed it and who in the organization got the e-mail first. This will help you warn people your organization deals with or find out how they handled it.
<input type="checkbox"/> Virus	What virus is it?	The machine you're using to make the connection needs to have one interface connected to the Internet, even if it's only a modem, and another connected to the internal network.
<input type="checkbox"/> Operating system	What e-mail software is your server running?	Different e-mail systems are affected by different viruses. For example, a virus that reacts one way on Outlook/Exchange may not affect GroupWise and GroupWise clients.
<input type="checkbox"/> Virus scanner	What virus scanner are you running?	You should know what virus scanner is running on both your e-mail server and your clients, in case you need emergency updates.
<input type="checkbox"/> Virus scanner	What do the virus protection makers say?	Check with the virus protection maker to see whether it has provided a patch for your virus and whether you need to obtain updates or patches.
<b>Communicate with end users</b>		
<input type="checkbox"/> Alternative communication	How do I communicate if e-mail is down?	Let users know that there's an e-mail virus attacking the network, but do so in a manner that doesn't cause panic. If need be, use instant messages or phone calls for notification. In a small organization, you may be able to personally deliver the warnings.
<input type="checkbox"/> Users	Who has been affected?	Find out who has been infected with the virus and who hasn't. It may help identify the source of the virus and how it's spreading in your organization.

**Stop the attack**

<input type="checkbox"/>	E-mail server	Do I need to bring down the e-mail server?	If the virus is spreading fast, you may need to immediately disconnect your e-mail server from the network.
<input type="checkbox"/>	Network	Do I need to bring down the network?	Some viruses propagate from client workstation to client workstation. If many clients are affected, you may need to bring down the whole network. The fastest way to do so may be by just shutting down hubs, routers, and switches in your organization. Warn users before doing this.
<input type="checkbox"/>	Virus scanner	Do I need updates or patches?	If you haven't recently obtained virus signature updates for the server, do so immediately using a machine that hasn't been infected. You may also need to download any special cleaning utilities the vendor has.

**Clean up the mess**

<input type="checkbox"/>	Virus scanner	How do I get rid of the virus?	Using the updated virus scanner or utilities you've downloaded, run them against the server and any affected workstations. You may need to use a utility like IISScan or ExMerge from Microsoft to physically delete infected messages.
<input type="checkbox"/>	Mailboxes	Do I need to recover mailboxes?	Some viruses damage user mailboxes. Make sure you have backups handy to recover the mailboxes.
<input type="checkbox"/>	Workstations	Do I need to reinstall client software?	You may need to completely reinstall the operating system, applications, and e-mail clients on client workstations. Make sure you have backups handy.

**Perform a postmortem**

<input type="checkbox"/>	Analysis	Who was affected?	Determine who was affected by the virus and, most important, find out the complete configuration of their workstations to discover whether there was any common security hole, such as an outdated security update or virus signature.
<input type="checkbox"/>	Analysis	Where did the attack come from?	Once you've determined the source of the attack, go to the source and find out whether they've made precautions to keep it from happening again.

- |                          |          |  |  |
|--------------------------|----------|--|--|
| <input type="checkbox"/> | Analysis | What viruses act the same way?           | Like biological viruses, computer viruses run in strains that are similar. Check security Web sites to find out whether there are any other viruses similar to the one you just faced.   |
| <input type="checkbox"/> | Analysis | How long did it take to fix the problem? | Document the amount of time it took to fix the problem. You may need this information for insurance purposes. Additionally, you may be able to cost-justify more staff or a different virus scanning solution if the one you had was inadequate. |

---

### Prepare for the next attack

---

- |                          |               |   |  |
|--------------------------|---------------|---|--|
| <input type="checkbox"/> | Virus scanner | Do I need to upgrade or replace my virus scanner? | Some applications don't work well through proxy servers or NATs. Check your application to see whether it will work before going to the trouble of installing a NAT.   |
| <input type="checkbox"/> | Users         | How do I educate users?                           | Make sure users know how to identify possible virus messages. Teach them to keep virus signatures up to date. Let them know the potential for data loss. Educate them using different approaches, including training sessions, e-mails, and newsletters.   |
| <input type="checkbox"/> | Education     | How do I keep up to date on threats?              | Sign up for updates from CERT, Microsoft, and antivirus software manufacturers about virus threats. Don't just count on getting all of the information from one source. You'll get lots of redundant information, but it's better than missing a potential attack.                               |
| <input type="checkbox"/> | Backups       | How important are backups?                        | Make sure you have regular, complete backups of your e-mail server. Rotate backups on the e-mail server just as you do on your file server. Encourage users to back up their software as well and to store personal mailboxes on a server share so the server backup software can access it too. |

# Address antivirus software in your disaster recovery plan

By Mike Talon

In this day and age, organizations must protect their systems against increasing virus attacks. However, organizations must consider how their antivirus software can impact the viability of their DR plans.

Potential virus attacks eliminate an organization's ability to ignore tape backups and other point-in-time data copies. While real-time replication of any form is a good idea for any business that can afford it, it should never be your only source of DR protection.

The reason is simple: If a virus attacks the primary server systems, it will replicate to the backup systems as well. The only way to prevent a virus that sneaks through your shield from wiping out your entire business is to create point-in-time data copies and store them in a safe place. Then, if a virus does attack, you can still restore from tape (or another point-in-time copy) if the virus manages to propagate to both the primary and backup systems.

In addition, antivirus software itself can impact your organization's disaster recovery strategy in two ways: during normal operation or in the event of a failover.

When systems are in normal operational order, you may employ antivirus software on both the primary and backup systems. On the primary systems, make sure the antivirus software doesn't cause any conflicts with replication tools, backup systems, and point-in-time versioning tools. Most software vendors make sure their software won't interfere with antivirus tools, so this isn't typically a big issue.

On backup systems, however, replication tools may conflict with antivirus software. This isn't the fault of either piece of software; rather, it's a consequence of the normal operation of both.

Replication systems send either block- or byte-level I/O operations to the backup server, which causes the antivirus software to scan the affected file. Since this can literally be a continuous procedure, an amazing amount of scanning can occur on the backup server's file system.

The easiest way to mitigate this issue is to use antivirus software that can exclude directories and files. Since the primary machine scans the files, it's fine if the scanners ignore those files on the backup machine. Another option is to use more powerful servers on the backup side, which could handle the increased activity.

Antivirus software can also impact your organization during a failover situation. When you switch to the backup server systems, you must ensure that the antivirus software switches with everything else during failover.

In many cases, you may not have installed and configured virus scanners on the backup systems, so you may have to perform these actions at failover. In other cases, you may have configured antivirus software to ignore certain directories and files.

To ensure proper protection, you must reenable those areas after failover. In any case, you must be absolutely sure the antivirus software moves along with the live server systems.

Antivirus software can have a substantial impact on a disaster recovery plan. Failure to plan properly for this issue can cause the failure of your DR plan—or worse, it can perpetuate a disaster all by itself. ❖

# Virus prevention Checklist

By Tanya Buba

Updated by Bill Detwiler

Recovering from a virus can be time-consuming and costly. To help you avoid such problems in the first place, we've assembled a checklist that includes options to consider when developing your virus prevention policies and plans. Of course, working environments differ, and it can be tricky to strike a balance between preventing viruses and hampering employee productivity. While a particular method may seem prudent to some IT managers, it may be viewed as too cumbersome and restrictive by others. But the possibilities on this list should help you determine which strategies will be the most effective for you and your end users.

## Thanks to TechRepublic readers!

These virus prevention methods are real-life examples of practices already in place. We compiled this list of suggestions based on input from our members and IT experts.

## Software and hardware configuration

- Schedule regular backups of your data files.

---
- Protect your servers (including e-mail and firewall servers) with antivirus software.

---
- Install antivirus software on all workstations.

---
- Enable the virus-detection option in CMOS.

---
- Install and appropriately configure a network firewall.

---
- Install and appropriately configure a software firewall on workstations, such as ZoneAlarm or Windows Firewall (Windows XP).

---
- Open only necessary ports on your firewall—pay particular attention to the ports used by FTP software and file sharing applications, such as iMesh, Kazaa, Gnutella, Morpheus, and Grokster.

---
- Perform regular port scans of your network to check for open ports.

---
- Lock down workstations to prevent users installing unauthorized software, such as unapproved e-mail clients, instant messaging programs, FTP clients, and peer-to-peer file sharing applications.

---
- If appropriate in your environment, set the attributes for critical system files (such as sys.ini, win.ini, autoexec.bat, and config.sys) to read-only to prevent them from being written to.

---
- Set permissions to the Windows registry and other system files to prevent unauthorized changes.

---
- Enable your antivirus software to alert you when your virus signatures are outdated.

- Configure servers to scan both incoming and outgoing files.
- Include all file types when scanning, such as exe, dll, and zip files.
- Consider using a software package that allows files to be quarantined. This will prevent users from gaining access to the infected files and perpetuating the virus.
- If productivity will not be compromised, consider disabling the A drive of high-risk workstations from within a password-protected CMOS. If this is not feasible, disable the option of booting from the A drive.
- Set an audible alert when viruses are detected.
- Set user response options to the minimal acceptable level, such as “Cure” or “Quarantine.” Do not give the user the option to “Cancel” the repair.
- Enable all macro virus protection within software packages, such as Word and Excel.
- Edit the file-exclusion list so all exe and dll files are included during scanning. Some viruses target these files specifically.
- Create and maintain a write-protected emergency boot disk and know how to use it.
- Create and maintain standard hard drive images for common workstation configurations. If a reformat is necessary, having an image on-hand will reduce down time.
- Remove internal workstation modems so that all machines must go through the corporate firewall.
- Don't use default/simple passwords on servers, network hardware, administrator accounts, and the like.
- Routinely check the corporate network for rouge servers installed by non-IT personnel.

### **Operating system and virus signature updates**

- Regularly install the latest client and server operating system security updates and patches. If appropriate in your environment, configure systems to automatically download and install updates.
- Schedule regular updates of virus signature files. If appropriate in your environment, configure your antivirus software to automatically update from the developers Web site or an internal server.
- Distribute the update to the workstations. If your NOS does not allow you to “push” updates to your users, consider sending it as an e-mail attachment.
- Consider setting up a dedicated server to retrieve your regular updates. Users can then connect to the internal server to update their workstations.
- Consider building the update into your users' network login script.

- Consider purchasing client management system such as Zenworks or Altiris if you have no other mass-distribution options available. These systems let you “push” updates to your workstations.
- Update your write-protected emergency boot disk whenever new signature files are received.
- Don’t rely on a single source for you security information. Regularly check multiple security Web sites and subscribe to security e-mail newsletters and alerts.

### **Removable media management (floppy diskettes, CDs, DVDs, flash media, etc.)**

- Avoid using data and program media received from unknown sources.
- Enact a policy that enforces the scanning of all unapproved media before it is used in a workstation.
- Consider providing a stockpile of virus-free diskettes for users to take home. Scan the diskette upon re-entry to the workplace to ensure that the user’s home PC is not infected.
- Write-protect all data and program diskettes.

### **Scanning**

- Consider using a dedicated workstation that continually scans data directories on the network.
- Schedule full workstation scans on a regular basis with minimal intrusion to the user, such as during lunch or after hours.
- Perform scanning in “stealth mode” to achieve minimal intrusion to the user.
- Disable user intervention of scans.
- Enable background monitoring/real-time scanning on all workstations.
- If available, user a browser plug-in to scan files prior to downloading.
- If a plug-in is not an option, make sure all downloaded files are scanned prior to installation.
- Smaller companies may want to document the date of the last “clean” scan of each workstation to alert the IT department at a glance.
- Scan new PCs received from vendors, as they have been known to contain viruses out of the box.

### **E-mail policies**

- Set e-mail server filters to eliminate spam and unsolicited junk e-mail that could contain a virus as well as malicious code.

- Set the server to immediately send a notification to the network administrator as well as the user. This will alert the user of the infected message before it is opened.
- Scan all incoming and outgoing e-mail and attachments.
- Discourage non-work-related downloading of attachments.
- Do not allow users to forward jokes or chain letter e-mail.
- Consider subscribing to a third party e-mail scanning service. Infected e-mail and attachments never enter your network.
- Call or e-mail the individual who sent the infected e-mail or document. They may not know they have a virus.
- Develop an alternate communication method in case e-mail fails.

### User policies

- Develop a system to educate all users about policies such as the “no download rule.”
- Require that all software installations be performed only by the IT department.
- Do not allow your users to download or install unapproved software, such as games and screensavers.
- Create a rule that users should not bring diskettes from home, unless they are willing to allow the diskettes to be scanned by the IT department prior to being used.
- Consider limiting Internet access to approved sites through a browser list or proxy server.
- Institute a set of applications that users have available to do their job. Do not allow any software to be installed beyond those provided with their system.
- Do not allow remote-access users to upload files to the network unless the IT department can verify the integrity of the PC being used for remote access.

### End-user education

- Publish links to reliable virus encyclopedias, such as the following:
  - o Computer Associates  
<http://www3.ca.com/securityadvisor/virusinfo/browse.aspx>
  - o F-Secure <http://www.f-secure.com/v-descs/>
  - o Kaspersky <http://www.viruslist.com/en/viruses/encyclopedia>
  - o McAfee <http://www.mcafeesecurity.com/us/security/vil.htm>
  - o Symantec <http://www.symantec.com/avcenter/>
  - o TechRepublic’s Virus Threat Center  
<http://www.virusthreatcenter.com/library.aspx>
  - o Trend Micro <http://www.trendmicro.com/vinfo/>

- Instruct your users to check these sites when they suspect they have a virus or when they want additional information. Users can also check for hoax virus information.
- Encourage users to install antivirus software on their home computers and require antivirus software on computers that remotely access the corporate network.
- Encourage users to store personal mailboxes and important files on a server share that you routinely backup.
- Encourage users to report when they find a virus on their system so you can track which viruses surfaced in your network.
- Consider developing an intranet site or Web site dedicated to virus information, with links to antivirus sites. If this is not an option, develop an e-mail newsletter that includes the same type of information.
- Inform your users of new virus threats. This will heighten their sense of awareness.
- Educate users on the proper use of macro virus protection. Instruct them to disable all macros when prompted unless the document has been given a clean bill of health and is known to be virus-free.
- Consider assigning offenders to an antivirus task force. Users found breaking policies or bringing a virus into the environment will be required to assist the IT Department in scanning workstations after hours.