# VirusBarrier
# User's Manual

VirusBarrier for Macintosh


Intego, Inc.

www.intego.com

# 1 - About VirusBarrier

## What is VirusBarrier?

VirusBarrier is the simple, fast and non-intrusive antivirus security solution for Macintosh computers, by Intego, the publisher of the acclaimed NetBarrier personal security software. It offers thorough protection against viruses of all types, coming from infected files or applications, whether on floppy disks, CD-ROMs, removable media, or on files downloaded over the Internet or other types of networks.

VirusBarrier protects your computer from viruses by constantly examining all the files that your computer reads and writes. With VirusBarrier on your computer, you can rest assured that your Macintosh has the best protection available against viruses of all kinds.

VirusBarrier is a Control Panel, which is automatically loaded when you start up your computer. It functions in the background, and checks everything that your computer does, looking for viruses. It knows the unique signatures of all known Macintosh viruses, and whenever a new virus is discovered, Intego's antivirus SWAT team goes into action to provide updated virus definitions, which you can check automatically using Intego's unique NetUpdate control panel

VirusBarrier was designed according to a few very specific concepts. The main idea is that, once it is installed and configured, an antivirus program should not require the user to do anything unless a virus is detected. The VirusBarrier philosophy can be summed up in three words: **simple**, **fast** and **non-intrusive**.

### Simple

VirusBarrier is the simplest, easiest-to-use antivirus program for Macintosh. After you install it, it works in the background, keeping a close eye on your computer, and verifies your files silently and efficiently.

### Fast

VirusBarrier is fast and effective. It does not slow down your computer, and you don't need to do anything while it works. Each time a file is written, used or opened, VirusBarrier checks the file to make sure it is safe.

### Non-intrusive

VirusBarrier is non-intrusive. It will not constantly ask you about "suspicious" activity, each time you install a program, nor will it generate endless "false alarms". Once you have installed it, you probably won't notice it is there, unless it detects a virus and alerts you. In addition, you do not need to deactivate VirusBarrier when installing new software, regardless of what the program's installer or manual may say. VirusBarrier can run all the time, in the background, protecting your computer without you needing to worry about it.

# VirusBarrier's Features

## Virus Scanning

VirusBarrier works in several ways. While it is constantly watching over your computer at all times, protecting you from viruses, it can also work in manual mode, and you can ask it to scan any disk, or shared volume on a network. VirusBarrier even searches for viruses inside Stuffit archives of compressed files.

## Automatic Repairs

If VirusBarrier is running in automatic mode, it will repair any infected files it finds by eliminating the viruses, if possible, or, if not, by indicating that the files are corrupted. In this mode, you can just forget about VirusBarrier's activity–you will only know it is there if it comes across any viruses or suspicious files.

## Manual Scan

You can also use VirusBarrier to manually scan your files. This is recommended the first time the program is installed, to make sure your computer is safe. You can then use it at any time to manually scan any disks or volumes to ensure that they are virus-free.

## Turbo Mode

VirusBarrier's Turbo Mode makes scanning much faster. The first time VirusBarrier scans your computer, it remembers all the files it examines. As long as these files are not updated, VirusBarrier will not rescan them, scanning from 5 to 40 times faster.

## Contextual Menu Module

VirusBarrier's contextual menu module allows you to quickly and easily scan a file, folder or volume on the desktop or in any window.

### Scan Logs

If VirusBarrier detects any infected or corrupted files, its Log will show you the names of these files, the viruses that they are infected with, and whether or not they have been repaired.

### Menu

The optional Intego menu in the menu bar gives you quick access to the VirusBarrier Control Panel.

### NetUpdate

VirusBarrier includes Intego's unique NetUpdate control panel, which allows you to check for program updates either automatically or manually. You can set the update frequency, so the program checks on a given day at a given time, every week. If you prefer updating the program manually, a simple mouse click connects you to the Intego server to check if there is a new version of the program.

### Virus Alerts

VirusBarrier allows you to set alert options so you can know if the program detects any viruses while working in the background. You can choose to have the program display an alert screen, play a voice message, or even send an e-mail message to a specific address. This can be useful if you want to run VirusBarrier on computers connected to a network and warn a network administrator, or the computer's owner when they are away from their computer.

### Password

VirusBarrier provides a password protection option. This can be very useful if you are administering a network, and want to ensure that users cannot change any of the settings you assign to the program. It can be set to ask for the password each time the program is

## Using this User's Manual

This user's manual provides detailed information on installing, using and updating VirusBarrier, as well as a complete encyclopedia of Macintosh viruses and a glossary of virus terminology.

You should start by reading the Introduction, to find out how computer viruses work (chapter 2), and then you should follow the Installation instructions (chapter 3). Next, you should read the description of VirusBarrier's functions (chapter 5), find out about VirusBarrier's Preferences (chapter 6), and if you want to know more about viruses you can consult the Virus Encyclopedia (chapter 9).

If you are having problems with your computer, and you think you may have a virus, you should read the Diagnosis section (chapter 7), for instructions on troubleshooting your computer, and determining whether you do, indeed, have a virus. If so, you will be instructed how to send any files that you think might be infected to Intego's Virus Monitoring Center so we can inspect them.

# 2 - Introduction to Computer Viruses

## Why You Need to be Protected

Your computer contains important information and files. If you use it for your work, you are aware how much time and money it would cost if you were to lose these files. Even if you use your computer just at home, you certainly have files you would hate to lose. On top of that, if a virus were to erase all of your files, even if you did not lose anything important, you would have to spend a great deal of time reinstalling your system and all of your programs.

An antivirus program is a kind of insurance policy. Of course, you imagine that you will never catch a computer virus, but if it did, you would be very unhappy. VirusBarrier is your insurance against all kinds of viruses—it watches over your computer so you don't have to worry about them

The virus threat is real. More and more viruses are being discovered every day. While the Macintosh is relatively privileged, compared to Windows, there is still the danger of existing viruses or new viruses spreading to your computer and damaging your files.

## What Is a Computer Virus?

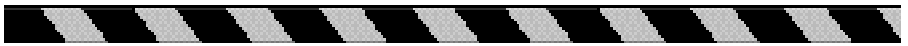
Nothing can scare a computer user more than suggesting that their computer may have a virus. They may react as though they, too, have caught a disease. Computer users have all heard the horror stories about what viruses can do, and, although some of them may be complacent, none remain indifferent when discovering a virus on their computer.

This is even more of a problem today, in our wired world, where people exchange files daily via e-mail. A virus on one user's computer can spread just as quickly as this year's flu epidemic. Yet, what exactly are computer viruses? How do they work? Why are they so dangerous?

The term virus was applied to computers for the first time in the early 1980s, when a self-replicating computer program was released "in the wild".

A virus is simply a bit of executable code that is attached to a file or application. Viruses don't get caught just from the air–they need a means of transmission, which could be a floppy disk, a CD-ROM, or a file sent over the Internet. Like viruses that invade our bodies, computer viruses attempt to replicate, after infecting a host, and attach themselves to more files and applications. They clone themselves, attack new hosts, and so on.

Viruses are basically small computer programs–the smaller the better, to hide more easily within files and applications and escape detection. They are written with only one purpose: to reproduce and spread among other computers. While some viruses do no damage, or merely cause a certain text to be displayed on-screen, most do indeed harm computers and files. There have been notable cases of viruses written without any malicious intentions, but, in most cases, viruses are written with the sole purpose of destroying files and propagating to other computers.



Computer viruses can infect any computer, from your home computer to your company's network, unless precautions are taken. The best precaution you can take is to use VirusBarrier, and, above all, make sure you keep it up to date.

## Who Writes Viruses?

In spite of what some people say, computer viruses are not written by the companies that sell antivirus programs. They certainly have enough work keeping up with the viruses that are in the wild without adding to them.

No one is really sure who writes viruses–angry teenagers, skillful hackers, who knows? Sure, some virus writers are arrested, but this is only the tip of the iceberg. The ones that are caught may actually want the attention they get from their viruses–many viruses have been found containing their author's name. Others are simply vandals, who get pleasure from seeing the havoc they can cause with their relatively simple programming. And still others are people who want to experiment, to see just how far their viruses can go in the wild, and how many computers will catch them. Or, are viruses simply, as one virus writer has said, "the electronic form of graffiti"?

There are even cases of viruses that had no "bad intentions", but, nevertheless, ended up causing many problems. One example of this is the MacMag virus, which tried to spread a message of world peace. (See chapter 9, the Virus Encyclopedia, for a description of this virus.)

Since the rise of the Internet, the real fear concerning viruses is no longer that one isolated individual might try and spread a virus just for attention, but that truly malicious people might use viruses to do economic damage on a large scale. Recent virus outbreaks, such as the LoveBug virus, have shown just how much it can cost, in lost productivity and down time, for a company to suffer a virus attack. If only for this reason, you should protect yourself in every way possible.

## How Computer Viruses Work

In the minds of most computer users, the term "computer virus" includes many types of "malware", not all of which are actually viruses: Trojan horses and worms, for example, work in different ways, and do not always replicate like viruses do, yet most people tend to include them as part of the virus family. While these programs are malicious, and can seriously damage your computer and your files, they function differently.

A real virus is a small bit of computer code, or programming instructions, that can be executed, or run, on the type of computer it targets. For this reason, viruses written to attack DOS and Windows computers have no effect on Macintosh computers, and vice versa. (Although, if you are running one of these operating systems in an emulator on your Macintosh, you will have to consider the vulnerability of the emulated system to any viruses that may target it.)

Viruses do two things when activated on a computer. First, they try and execute their code, in order to do the damage they were designed for, and then they try to reproduce themselves, by copying this code into other files, applications, disks or network volumes. Here is an example of what a fictional virus might do on your Macintosh. (Actually, this example presents the actions of a Trojan horse, since it will be easier to understand.)

> You receive an infected program from a friend, or customer, over the Internet. Even though you have been told not to open e-mail attachments that come from people you don't know, this comes from someone you trust, so you open it. Let's assume that it is an application, say, an animated greeting card. You double-click the file, and the application starts running. While it is running, however, it sets off its viral code, and alters your System file. It copies malicious code into your System, and, at the same time, searches your company's local network for other System files, and copies itself there as well. After the presentation is finished, you quit the application. Nothing happens to your computer right away, though,

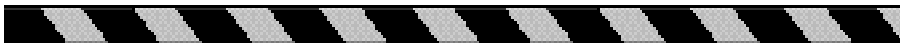
since the code is set to truly act only when you restart your computer.

The next morning when you get to work, and start up your computer, you notice it takes longer than usual to start. When it finally starts, you find that it is running very slowly. When you go to open that urgent report that has to be finished by lunchtime, you notice the file is no longer there. You look through your hard disk, and find that dozens, even hundreds of files are missing. It is then that you realize that you forgot to back up your computer yesterday, and have no copies of any of these files.

In the meantime, you have already sent the animated greeting card to some other friends, but you don't make the connection between the greeting card and your missing files. It is only several hours later, when one of your friends calls, that you realize this, since he discovered that the animated greeting card did something to his computer.

As you see, this simple viral infection can have very serious consequences. Not only for you, but also for those you are in contact with. One of the biggest problems with viruses today is that computer users are constantly sending files to one another over the Internet, and computers can get infected much more quickly than in the past, when files were only sent on floppy disks. By protecting yourself with VirusBarrier, you are also protecting others.

Anyone who watches the news or reads the paper is aware of the recent computer viruses that traveled around the world in less than 24 hours. While these high-profile viruses, such as the Melissa and Love Bug viruses, affected Windows computers using specific software, there is no reason why similar viruses could not be targeted to Macintosh computers.



## Different Types of Viruses

Viruses can be broken down into two different types, according to what they target in your computer. The first type is called system viruses, since these viruses attack the System file, extensions, or the Desktop file. The second type, file viruses, infects applications, data files, or even control panels and extensions.

### System Viruses

System viruses are the most dangerous of all, since they can damage the operating system itself. We are also including in this section two other types of malware: Trojan horses and worms. While not technically the same as system viruses, they tend to act more globally than file viruses.

### Viruses

A computer virus is a small program that acts like a parasite, living in a host file or program, that is capable of infecting files and applications, reproducing itself, and spreading to other computers through infected files and applications. It is no surprise that people use terms originally used for diseases to speak of computer viruses–they work in a very similar manner.

Viruses that attack your system are among the most lethal. The damages they can do are such that you may need to reinstall your system entirely, and even reformat your hard drive and check all your backups to make sure they are disinfected.

Some of these viruses, such as the CDEF or WDEF viruses, only infect the Macintosh's Desktop files. These are invisible files that keep track of which icons go with which types of files and applications. These viruses, which do not affect other files, spread extremely quickly, since the first thing your Macintosh does when mounting a disk or volume is read its desktop files.

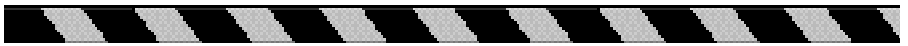
Other system viruses, such as versions of the SevenDust virus, can infect System files, control panels and applications, and, at a certain time, on a certain date, delete all non-application files on your startup disk.

Some viruses act very quickly, while others are set to go off at a certain time. Some merely content themselves with spreading to other disks and volumes, but all system viruses can potentially cause damage.

## Trojan Horses

The name Trojan Horse comes from an episode in the war that opposed the Greeks and the city of Troy, more than two millennia ago. It was a huge, hollow wooden horse that the Greeks built and gave to the Trojans, apparently as a gift, before supposedly sailing away and ending the war. While some of the Trojans were skeptical about it, the horse was taken inside their stronghold. That night, Greek warriors emerged from the horse, opened the city gates, and Greek soldiers from outside stormed the city.

It is obvious that the Trojans were never told not to open attachments. The Trojan horses that we are worried about are programs that look innocent, and claim to do a certain task, but, in reality, contain malicious code or viruses. In many cases, Trojan horses can be even more dangerous than other viruses. Some examples are ChinaTalk, which looks like a system extension but deletes folders, or the famous MacMag Trojan, which infected System files.



## Worms

Worms are one of the oldest form of viral programs on computers. They spread by methods other than attaching themselves to files and applications, and can be very difficult to find. The most recent serious worm on the Macintosh, called the AutoStart worm, created invisible files that could destroy data and files.

Worms use system functions to spread–the AutoStart worm spreads from infected CD-ROMs using the MacOS Autoplay function. It creates invisible extensions that activate each time the computer is restarted.

## File Viruses

File viruses are different from system viruses in that they attach themselves to data files, rather than applications, and their hosts depend on specific programs to do their damage. Recent examples of file viruses, that targeted Windows computers, were the very damaging Melissa and LoveBug viruses. These viruses came in attachments, which, when opened, activated certain functions built in to Microsoft applications under Windows. In a way you could think that these were Trojan horses, but the difference is that a Trojan horse is an application which purports to do a certain task, whereas these file viruses were actually code embedded in files.

## Macro Viruses

Most file viruses are macro viruses. This family of viruses poses the greatest threat for Macintosh users today.

The first real macro virus that was found in the wild was the Concept virus, which attacked Microsoft Word files. This was quickly followed by other variants, as virus writers saw the potential to do great damage through the ubiquity of this program. Later, macro viruses were written to exploit

Microsoft Excel as well. In just 5 years, since the appearance of this first virus, several thousand macro viruses have been found.

The real danger of macro viruses is the fact that they are the first cross-platform viruses. For years, Macintosh users could be relatively secure concerning viruses, knowing that there were only a few dozen viruses that targeted Macintosh computers, compared to thousands for Windows. But, now that macro viruses are prevalent, there is a real and present danger.

Many programs provide the ability to create macro commands. These simple programs use either the internal functions of an application, such as AppleWorks, to "record" and "play back" commonly used sequences of commands. Other applications, such as Nisus Writer, provide a more powerful macro language, which includes both menu commands and a programming language. Programs such as Microsoft Word and Excel base their macro functions on Microsoft's Visual Basic, which is similar to the Basic programming language.

One of the reasons that macro virus writers target Microsoft programs is that these applications allow users to embed macros in data files. In the past, one worried only about viruses coming through applications, since, for a virus to act, it has to execute, and only applications could execute. But the Microsoft Visual Basic approach is different–if you wish to use a macro, you can either run it from your template or add it to a data file. This surprised users, at first, since they thought that nothing was "executed" when opening a word processor or spreadsheet file. But these files can, indeed, contain "programs", and do things you would never expect.

If the macro language provides the possibility to modify files, a macro virus will be able to copy itself into other files used by the same application. This then allows the virus to spread when you open other files, create new files, or pass files on to someone else.

Most macro viruses that target Microsoft Word files use commands such as AutoOpen, AutoClose, AutoExec and AutoExit. These are commands that are executed when a certain event occurs to the file, and these four

events are those which always occur when you work with a file. If, for example, a macro were written to copy itself only when you choose a certain menu command, it would be far less certain of spreading.

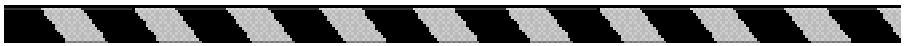
The most common action for macro viruses is to act when a file opens, and, first, copy themselves into the template that is opened as well. You don't physically open this template, but it is always open in the background–it contains certain customization information, such as toolbars, as well as any legitimate macros you may have added to it.

The most prevalent macro virus that affects Microsoft Word copies itself into the active template, changes some menu items, so you cannot edit the template, changes file types (which changes their icons, turning them into templates themselves), then copies itself from the corrupted template into all new files you create or open. This virus can be removed, if caught in time, by removing the active template file and any infected files.

Other macro viruses can be much more dangerous. They can corrupt or delete your files, hide certain application functions, and even more. And, on top of all that, they are cross-platform viruses, which can do damage both to Macintosh computers and PCs running Windows.

It is important to note that macro languages are very powerful tools that can be extremely helpful. Not all macros are viruses. While Word 98 includes a function to alert you if there are macros in any documents you open, this defeats the purpose of having a macro function. The real problem is that the macros are stored in data files, rather than, say, in separate macro files (some applications, such as Nisus Writer, do this). Users could easily exchange macros, and be certain that the files they open contain only data. Unfortunately, this approach to a macro language leads users to be far too worried about macros, instead of using them for their function-enhancing properties.

VirusBarrier detects all known Word and Excel macro viruses, and is constantly updated when new macro viruses are found.



## Hoaxes

Hoaxes, that is, e-mail messages or newsgroup posts warning people about non-existent computer viruses, are a growing problem. While they are not viruses themselves, they do tend to reproduce in a similar way–worried users forward these messages to their friends and co-workers, thinking they are true, thus making them worry unduly about some imaginary virus.

One of the most widespread hoaxes is called Good Times. This virus takes its name from the subject of the e-mail message that is supposed to contain a virus. You might think that if it were clearly such a hoax it would have not lasted very long, yet the Good Times "virus" message is still seen many years after its first appearance in 1994. Other copycat hoax messages are regularly circulated around the Internet as well, and you have probably already seen at least one, if not more.

These hoaxes capitalize on the lack of computer knowledge of most Internet users. It is true that they always sound serious, and sometimes seem to be forwarded from major computer companies. Yet they are all jokes, although not very funny ones.

If you receive a message like this, and you are worried that it might not be a hoax but a real virus alert, the first thing you should do, if you work in a company, is contact your system administrator to find out if it is real. If you are a home user, you can always check the Intego web site at www.intego.com. If there are any new viruses around that you need to worry about, we will post information on our web site as soon as possible. Intego's Virus Monitoring Center is ready 24 hours a day, 7 days a week, and will react on the first signs of any new viruses.

If you think you have caught a new virus, see chapter 7 for instructions on how to diagnose your computer, and how to contact Intego's Virus Monitoring Center.

## How do Viruses Spread?

Viruses can spread in a few basic ways. They can only infect two things–files, or storage media. Media, such as floppy disks, CD-ROMs, etc., for the Macintosh, contain invisible files called Desktop files. These files contain information for the System concerning file icons and applications. Viruses that infect Desktop files can spread when your computer reads these removable media, since the first thing your Macintosh does when mounting a disk or volume is read its desktop files. VirusBarrier protects your computer from these viruses by scanning all Desktop files in removable media, before viruses have a chance to spread. If VirusBarrier detects a virus in these Desktop files, it will disinfect them before your computer finishes reading the files.

The other way viruses can spread is through infected files. These files may be on floppy disks, CD-ROMs, or downloaded from the Internet. They can also be sent as attachments via e-mail. Infected files cannot spread their viruses without being opened or read. Merely copying an application cannot cause a virus to spread, but starting up that application can. The same goes for data files–if you happen to receive a file with a macro virus, there is nothing to worry about as long as you don't open the file. VirusBarrier protects your computer from these viruses by scanning files on your computer when they are written, used or opened. As soon as you do something with a file, it is scanned immediately, and if VirusBarrier detects a virus, the file or application will be disinfected, or rendered inoperable.

## How Can You Protect Yourself from Viruses?

There are a few simple ways you can protect yourself from computer viruses. The first, and certainly the most important, is to use VirusBarrier to constantly monitor your computer and automatically check for viruses. VirusBarrier provides the best protection for your Macintosh, and works in the background, to ensure that your computer remains safe.

To ensure that VirusBarrier is always watching out for all known viruses, you must update the program regularly. Intego's NetUpdate control panel makes this easy to do, even automatic, if you choose. You should check for updates at least once a month, and you can even check the Intego web site (www.intego.com) from time to time to see if there are any new viruses that require a more immediate update.

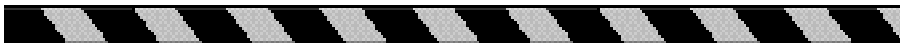
Another very important point is that you should only use software that comes from reputable sources. Pirated software may contain viruses, or may be an unexpected Trojan horse. Only install software if you are sure of where it comes from. VirusBarrier protects you by checking each file as you install software, making sure that they are safe.

In addition to this, you should be very wary of files sent by e-mail or over the Internet. We have seen how the oldest recorded case of nonchalantly opening an attachment led to disastrous consequences (when the Trojans opened the horse given to them by the Greeks). People used to say that you should never open attachments from people you don't know, but recent viruses on Windows computers have spread because the virus was in attachments that came from friends and co-workers. In any case, if you get an attachment from someone you don't know, you are best not opening it. But this does not ensure that your colleagues are not unwittingly spreading viruses in their files. VirusBarrier protects you by scanning every file as you open it, and eliminating all known viruses automatically. If you are on a network, and VirusBarrier detects a virus in an attachment, make sure you contact your network administrator immediately, so they can remove the infected file from your company's mail server.

In spite of all the antivirus protection provided by VirusBarrier, there still remains one additional thing you should do to protect your data: back up your files regularly. Not only should you back up important files every day, but you should also make multiple backups of them. The media you use for backups could get damaged or corrupted, and, in this case, your backups won't be much use.

A good way to work is the following: say you use a Zip drive to back up

your files. You should use at least two different Zip cartridges for your backups, changing each day. Think of this as insurance. Not only does this ensure that you have clean copies of your files if you find a virus on your computer, but it also protects your data from any other types of problems, such as hard disk crashes, etc. Given the relatively low cost of removable media, or even writable CD-ROMs or external hard disks, you should also back up your System and applications as well, although you don't need to do this as often. Remember, if, for some reason, your computer gets corrupted, it will take you a long time to reinstall your system and applications. If you back up your entire computer, you will be able to do this in just a few minutes.



# 3 - Installation

## System Requirements

- Any MacOS compatible computer with a PowerPC processor
- Mac OS 8.0 or higher
- 16 MB RAM
- 8 MB free hard disk space
- CD-ROM drive
- Minimum screen resolution 640 x 480 or higher
- Display: thousands of colors

## Installing VirusBarrier

Installing VirusBarrier is very simple. Insert the VirusBarrier CD-ROM in your computer's CD-ROM drive. A window will open, containing the VirusBarrier installer, the Read me file, the VirusBarrier manual (this file), and an Acrobat Reader installer.


First, double-click the VirusBarrier installer.

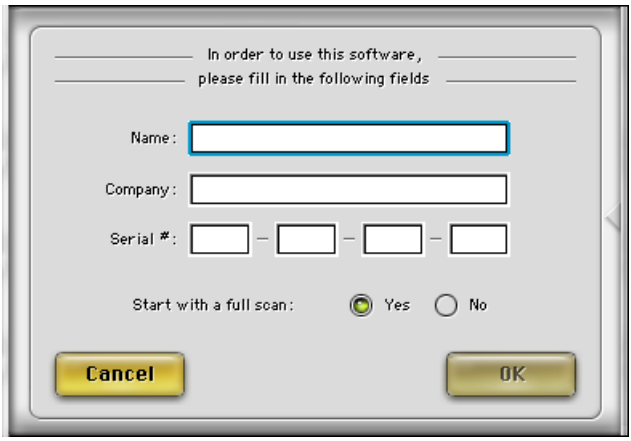
You will see a window displayed containing the VirusBarrier license. Read this license carefully, and, if you accept it, click on Accept.

The following window will be displayed:


Click on Install to install VirusBarrier. VirusBarrier will be installed, and, after the installation is complete, you will be instructed to quit the installer. Your computer must be restarted for the Intego menu to be displayed in the menubar, but VirusBarrier will start watching over your computer right away.

## Registering VirusBarrier

VirusBarrier will now display its Registration window:




You must enter your name, company, if any, and your serial number. The serial number is found on a sticker on the VirusBarrier CD box, is made up of four groups of four characters, and is not case-sensitive.

This window also asks you if you want to have VirusBarrier run a full scan of your computer after installation. You should select Yes to this option, since it is best to ensure that your computer is safe and clean right away.

When registration is completed, VirusBarrier will open its control panel, and you can configure the program.

### Uninstalling VirusBarrier


To uninstall VirusBarrier at any time, run the installer, and select Uninstall from the popup menu.

# 4 - Quick Start

## VirusBarrier's Default Mode

When you install VirusBarrier, it automatically begins watching over your computer. VirusBarrier is designed to be simple and non-intrusive, and it fully protects your computer without your doing anything at all.

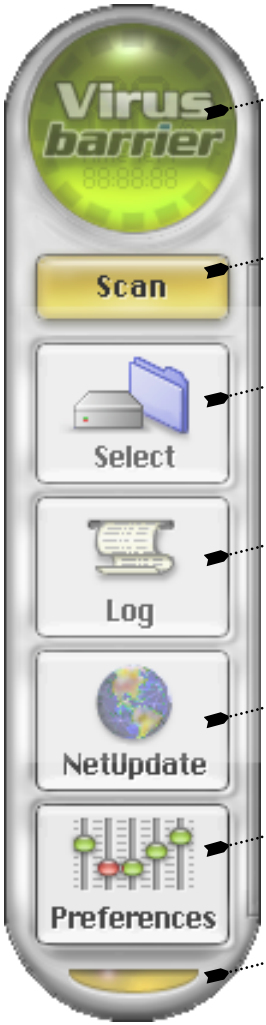
Once the program is installed, you can just let it run on its own. However, it is recommended that you either set the NetUpdate control panel to make automatic checks, to find if the program has been updated, or that you make manual checks, at least once a month.

To open VirusBarrier, and change any of the settings, or run a manual scan, select the Apple menu Þ Control Panels Þ VirusBarrier.

You can also open VirusBarrier by selecting VirusBarrier from the Intego menu in the menubar.

## VirusBarrier Interface

The VirusBarrier control panel looks like this. It contains the Orb, the contextual control button, and several other buttons, for choosing settings or running scans.




**The VirusBarrier Orb.**
This gives you information concerning the current operation.

**The contextual control button.**
This button changes according to the function it can have, such as Scan, Pause, Stop etc.

**The Select button.**
This button lets you select a volume, folder or file to scan for viruses.

**The Log button.**
This button opens the VirusBarrier log, showing any infected or corrupted files found during a scan.

**The NetUpdate button.**
This button opens the NetUpdate control panel.

**The Preferences button.**
This button lets you choose VirusBarrier settings.

**The About button.**
This button gives you information about VirusBarrier.

## Using the VirusBarrier Interface

To access any of VirusBarrier's functions, click on one of the buttons on the interface, and a drawer will open.

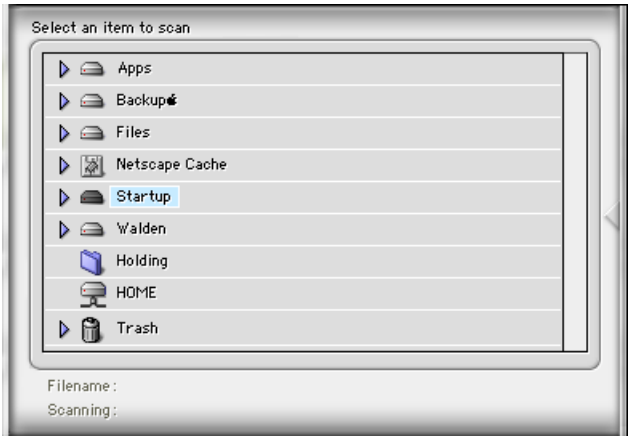

To close the drawer, click on the same button or on the triangle at the right of the drawer. You can also click on another button to close the current drawer and open the drawer corresponding to the other button.

## Running a Manual Scan

Once VirusBarrier is installed, it watches over your files, ensuring that they are safe from viruses. But VirusBarrier checks files as they are read, used or written. The installation procedure gives you the option to run a manual scan of all your files right after installation, to make sure that your entire computer is disinfected. You should do this, to make sure that you don't have any infected files. After that, VirusBarrier makes sure that all the files you use, copy, write and save are free of viruses.

If you did not choose to run a full scan after installation, or if you wish to run a manual scan at any time, open the VirusBarrier control panel by selecting the Apple menu Þ Control Panels Þ VirusBarrier. You can also open VirusBarrier by selecting VirusBarrier from the Intego menu in the menubar.

Click the Select button, and a drawer will open showing all of the volumes currently mounted on your computer. This view is similar to a Finder list view, showing volumes, folders and files according to their hierarchy. To expand a volume or folder, and view its contents, click the triangle to its left, and all the files and folders it contains will be displayed below it. To collapse an open volume or folder, click the triangle to close it.



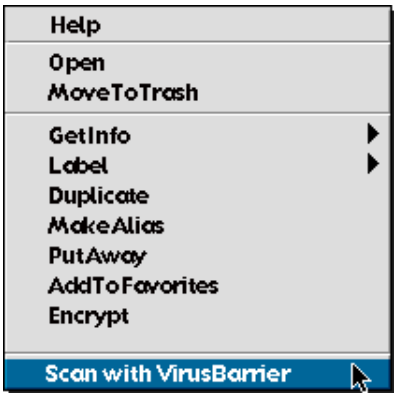

To run a manual scan on any of your volumes, folders or files, double-click the item you wish to scan, or click it once to select it, and click the Scan button. You will see from the activity in the Orb that scanning has begun. The Orb first displays the time required for the scan, under the words "Counting", as VirusBarrier counts how many files are to be scanned, then it displays the number of files scanned, under the text “Scanned”. The percentage of files scanned is shown at the top of the Orb, and if you click the Orb, the "Scanned" will change to "Files left", and show the number of files remaining to be scanned.


You can stop the scan at any time by pressing the Stop button. If you wish to pause the scan, hold down the Shift key on your keyboard, and you will notice that the Stop button now displays Pause. Click this button, and scanning will pause.


To resume scanning, click this button, which now shows Resume.

## Scanning Files with the Contextual Menu

VirusBarrier has a contextual menu module, which allows you to quickly and easily scan a file, folder or volume on the desktop or in any window. To do this, merely hold down the Control key and click on the item you wish to scan (or click the right button of your mouse, if you have a two-button mouse that is set to display a contextual menu) and select Scan with VirusBarrier. The file, folder or volume will be scanned, and you will be alerted if any viruses or corrupted files are found.



## The VirusBarrier Menu

When VirusBarrier is installed, it places a menu with the Intego icon in your menubar.


This menu can be used for two things: you can open the VirusBarrier control panel, by selecting VirusBarrier from the menu, and you can open the NetUpdate control panel, to check for updated versions of VirusBarrier, or to set NetUpdate preferences. See the NetUpdate User's Manual for more on NetUpdate and its preferences.

# 5 - VirusBarrier Functions


VirusBarrier is a powerful easy-to-use program that protects your computer from all types of viruses. It works in the background, providing you silent and efficient protection all the time.

## Virus Scanning

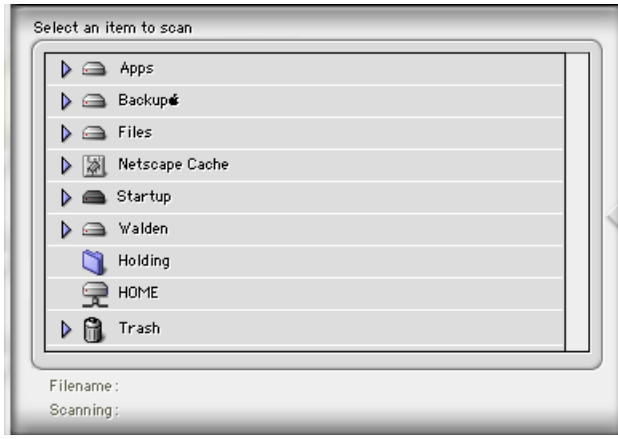
VirusBarrier works in several ways. It constantly watches over your computer at all times, protecting you from viruses. It can also work in manual mode, allowing you to scan any computer, disk, or volume on a network.

## Manual Scans

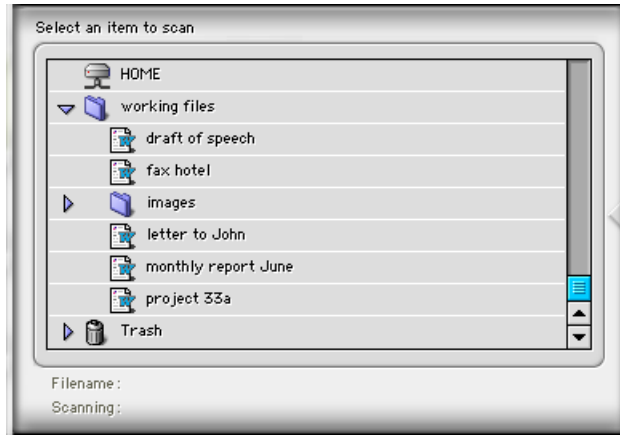
The first time you use VirusBarrier, you should run a manual scan on all of your computer's hard disks, or volumes. This ensures that there are no viruses hiding on your computer. This can be done automatically after program installation. To find out how to do this, see chapter 3, Installation.

You can also run a manual scan on any volume, folder or file, at any time. To do this, open the VirusBarrier control panel, and click the Select button.

A drawer will open showing all of the volumes currently mounted on your computer. This view is similar to a Finder list view, showing volumes, folders and files according to their hierarchy.


To expand a volume or folder, and view its contents, click the triangle to its left, and all the files and folders it contains will be displayed below it.




To collapse an open volume or folder, click the triangle to close it.

## Scanning a Volume



To scan a volume, just double-click it, or click it once to select it, and click the Scan button. You will see from the activity in the Orb that scanning has begun. The Orb first displays the time required for the scan, under the words "Counting", as VirusBarrier counts how many files are to be scanned, then it displays the number of files scanned, under the text “Scanned”. The percentage of files scanned is shown at the top of the Orb, and if you click the Orb, the "Scanned" will change to "Files left", and show the number of files remaining to be scanned.

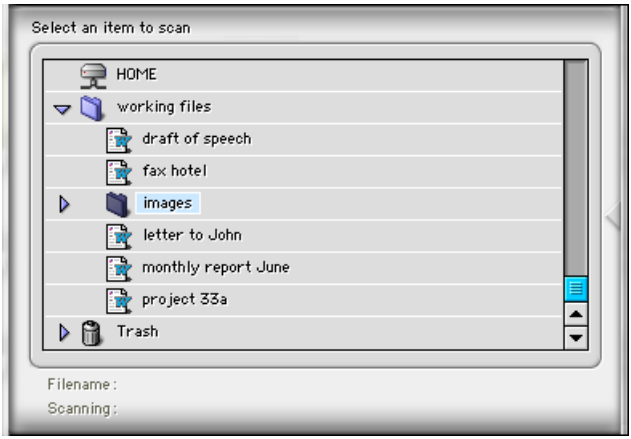


You can stop the scan at any time by pressing the Stop button.


If you wish to pause the scan, hold down the Shift key on your keyboard, and you will notice that the Stop button now displays Pause. Click this button, and scanning will pause.


To resume scanning, click this button, which now shows Resume.

## Scanning a Folder





To scan any folder on your computer, click the triangle at the left of a volume, and navigate in this manner until you find the folder you want to scan. Double-click this folder, or click it once to select it, then click the Scan button. You will see from the activity in the Orb that scanning has begun. The Orb first displays the time required for the scan, under the words "Counting", as VirusBarrier counts how many files are to be scanned, then it displays the number of files scanned, under the text “Scanned”. The percentage of files scanned is shown at the top of the Orb, and if you click the Orb, the "Scanned" will change to "Files left", and show the number of files remaining to be scanned.

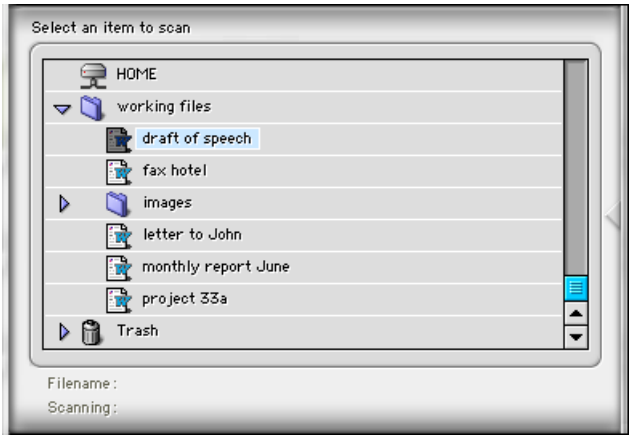


You can stop the scan at any time by pressing the Stop button.


If you wish to pause the scan, hold down the Shift key on your keyboard, and you will notice that the Stop button now displays Pause. Click this button, and scanning will pause.


To resume scanning, click this button, which now shows Resume.

## Scanning a File





To scan any file on your computer, click the triangle at the left of a volume or folder, and navigate in this manner until you find the file you want to scan. Double-click this file, or click it once to select it, then click the Scan button. You will see from the activity in the Orb that scanning has begun. In most cases, if you are scanning just one file, the scan will be completed almost immediately.

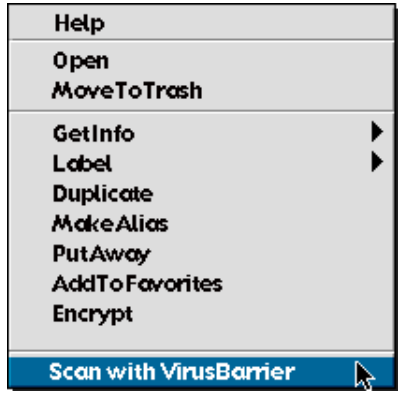

### Drag and Drop Scanning

You can also scan any volume, folder or file by dragging it on to any part of the VirusBarrier interface. Once you release the item to be scanned, VirusBarrier will start scanning it, the same as for any other manual scan.

## Scanning Files with the Contextual Menu

VirusBarrier has a contextual menu module, which allows you to quickly and easily scan a file, folder or volume on the desktop or in any window.

To do this, merely hold down the Control key and click on the item you wish to scan (or click the right button of your mouse, if you have a two-button mouse that is set to display a contextual menu) and select Scan with VirusBarrier. The file, folder or volume will be scanned, and you will be alerted if any viruses or corrupted files are found.



## Scan results


If VirusBarrier finds any infected files, the Log window will open, showing the names of any infected files, and the type of viruses they are infected with. If you have asked VirusBarrier to scan only, and not repair, any infected files will be shown here, and the type of viruses they have. If VirusBarrier is set to repair files automatically, you will see the names of any repaired files, and what type of viruses they had.

## Understanding Scan Results

VirusBarrier will inform you if it finds any files infected by any known viruses. It will also alert you if any corrupted files are found.


If any infected files are found, the VirusBarrier Orb will turn red, and the Log drawer will open. This drawer will open as soon as an infected file is found, so the scan may still be going on when this drawer opens. VirusBarrier will also alert you, according to the alert options you have set in the Preferences. For more on alert options, see chapter 6, VirusBarrier Settings.

The display in the Log drawer will also depend on the Scan mode you have selected in the Preferences. You have the choice between having VirusBarrier make automatic


repairs (Repair mode), or merely alerting you when infected or corrupted files are found (Scan mode). If you have chosen Repair mode, repairs will be made immediately, if possible. If you have chosen Scan mode, repairs must be made manually. For more on Repair mode and Scan mode, see chapter 6, VirusBarrier Settings.

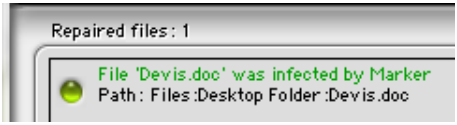

If you have chosen Scan mode, the Log drawer will show the name(s) of the infected file(s).

To repair a file or files, select the item(s) you wish to repair, and click the Repair button under the Orb. The file will be repaired, and the Log drawer will show this change.

## Corrupted Files

If any corrupted files are found, the VirusBarrier Log drawer will open. This drawer will open as soon as a corrupted file is found, so the scan may still be going on when this drawer opens. VirusBarrier will also alert you, according to the alert options you have set in the Preferences. For more on alert options, see chapter 6,

VirusBarrier Settings.




Corrupted files may not contain viruses, but many viruses can corrupt files, even if they do not copy themselves to these files. These files could also have been corrupted by such things as disk errors, or crashes when files are open. If any corrupted files are found, you should replace them as soon as possible.

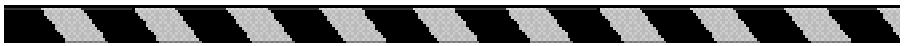

## Alerts

While VirusBarrier can be used to run manual scans, as seen above, it usually works in the background. It has several ways of alerting you if it finds any infected files.

If VirusBarrier detects any infected files, and you have set it to scan, and not automatically repair infected files, it will display an alert.


If you want VirusBarrier to repair the file, click Repair. If not, click Ignore. The file will not be repaired. Warning: this can be dangerous! Only select to not repair files if you are sure of what you are doing!

For more on setting Alert preferences, see chapter 6, VirusBarrier Settings.



# 6 - VirusBarrier Settings

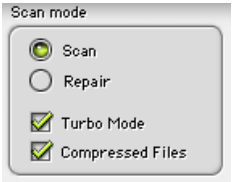
# VirusBarrier Preferences


## Preferences

If you click the Preferences button on the VirusBarrier interface, you can set several different options. You can set the scan mode, whether the program scans or repairs; you can set a password; and you can set several alert options.

You can also open the Preferences drawer by selecting Preferences... from the Edit menu.

## Scan Mode




VirusBarrier lets you choose between two virus scanning modes: Scan mode and Repair mode. If you select Scan mode, VirusBarrier will alert you any time it finds infected files, but will not automatically repair the files by disinfecting them. If an infected file is found, VirusBarrier will alert you, or, if you are running a manual scan, the Log will display the infected file, but you will need to repair the file manually. This may be useful if you are on a network, and your network administrator will need to examine any infected files you might find.

To select the Scan mode you wish to use, click the appropriate radio button.


## Turbo Mode

If you check the Turbo Mode check box, VirusBarrier will scan your files more quickly. The first time VirusBarrier scans your computer, it remembers all the files it examines. As long as these files are not updated, VirusBarrier will not rescan them, scanning from 5 to 40 times faster. However, if any of these files are modified they will be scanned. Also, when updating VirusBarrier for new virus definitions, all files will be scanned to ensure that all your files are free of all known viruses.

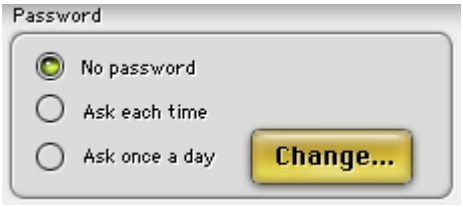
## Compressed Files

If you check Compressed Files, VirusBarrier will scan compressed files contained in Stuffit archives. You must have the Stuffit Engine installed on your computer (this is installed with Mac OS 9, or available with the free Stuffit Expander from www.aladdinsys.com). When scanning compressed files in Stuffit Archives, you will see a dialog box displayed briefly as the archive is examined, and any infected or corrupted files contained in an archive will be signaled. To repair or disinfect these files, you will need to decompress the archive, repair or disinfect the files by dragging them (files or folder) onto the VirusBarrier orb, or selecting them using the VirusBarrier contextual menu, and delete the original infected or corrupted archive.

## Using a password with VirusBarrier

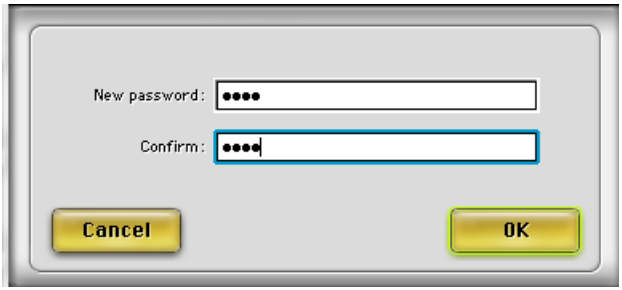
VirusBarrier has an additional level of protection, to prevent other users from making changes to your settings. You can set a password in VirusBarrier, and several options allow you to choose how VirusBarrier will work with this password.

## Creating a password





To create a password, click on Create... A dialog box will be displayed, asking you to enter a password.




Type your password in the first field, then type it again in the second field for confirmation. (Your password must be at least 4 characters long.) The password will be hidden.

If you wish to validate this password, click OK; if not, click Cancel.

## Password options


There are three options as to how VirusBarrier will request that you enter your password.

### No Password

If you check this option, after setting a password, VirusBarrier will not ask you to enter your password. This is useful if you have set a password, but want to deactivate the password protection temporarily. Your password will still be saved, but you will only be asked to enter it if you check one of the other two options.

### Ask each time

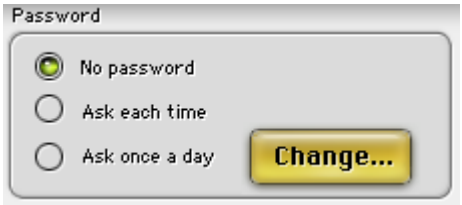
If you check this option, VirusBarrier will ask you to enter your password each time it is opened, or each time an alert is displayed. This offers total protection, but will require you to enter your password more often.

### Ask once a day

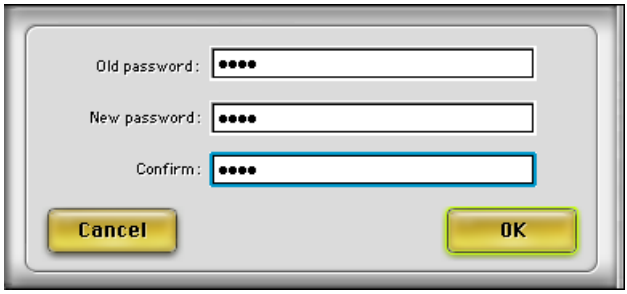
If you check this option, VirusBarrier will ask you to enter your password once each day. You will be asked the first time VirusBarrier is opened, or when an alert is displayed, and then you will not be asked again until the following day.

### Changing your password

If you have entered a password in VirusBarrier, there will now be a Change... button on this panel.



To change your password, click the Change... button, and enter your old password, then enter a new password and confirm it.

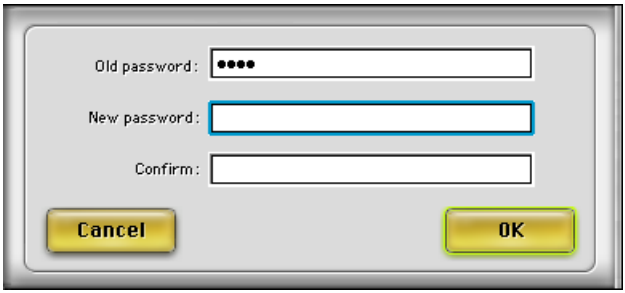



If you wish to validate this new password, click OK; if not, click Cancel.


## Erasing your password

If you have already entered a password, and wish to erase it, begin by clicking the Change... button.

To erase your password, click the Change... button, and enter your old password, and enter nothing in the new password fields.




If you wish to validate this change, click OK; if not, click Cancel.


## Alerts

This drawer gives you several options as to how VirusBarrier will act when presenting an Alert.


### Alert options

You have a choice between two actions, when VirusBarrier detects infected files. If you check Repair, all infected files will be automatically repaired. If you check Ask, an alert will be displayed asking you if you wish to repair the infected file.

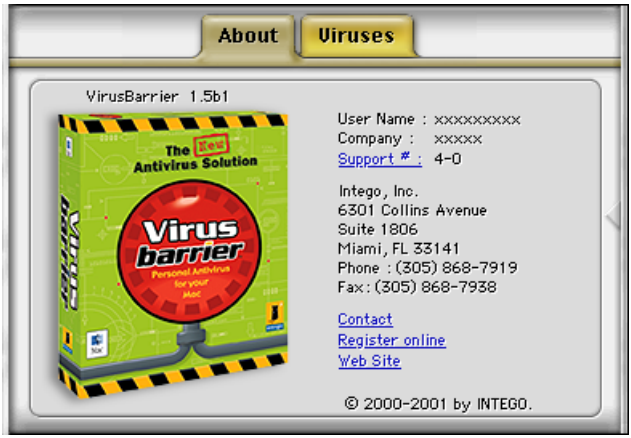
### Play sound to notify

If this is checked, VirusBarrier will play a synthesized voice indicating whether there are any infected or corrupted files, or not.

### E-mail

If this is checked, and VirusBarrier is not in the background, it will automatically send an e-mail message to the address entered in the text field. You must also enter your SMTP server in the second field.

## About VirusBarrier





The first tab in this drawer, About, gives information about VirusBarrier, such as the version number, your support number (a number you will need for technical support), clickable links to Intego's web site and e-mail address, and Intego's address and telephone number.

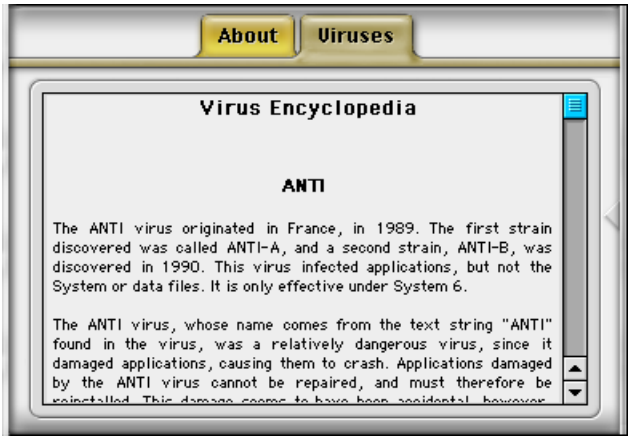
If you wish to contact Intego with any questions, click the Contact link, and your e-mail program will create a new message to Intego, with a subject "message from client #" followed by your client number. You can then type the text of your message, and send it to Intego right away.

If you need to contact Intego for technical support, click the Support link. Your e-mail program will create a new message to Intego, with a subject "support message from client #" followed by your client number. You can then type the text of your message, and send it to Intego right away.

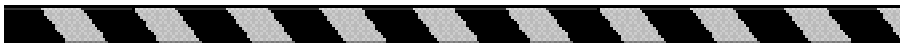

Clicking the Register online link will take you to the VirusBarrier registration page on the Intego web site. It is important to register your software, so Intego can keep you up-to-date on the latest information concerning VirusBarrier, Intego and its other products.

Clicking the Web Site link will take you to the Intego web site.

## Virus Encyclopedia




The second tab in this drawer, Viruses, contains a Virus Encyclopedia, with a complete history of many of the Macintosh viruses that VirusBarrier protects you from.



# 7 - Diagnosis

# If You Think You Have a Virus

## Some Symptoms of Infection

While the presence of these symptoms does not necessarily mean that a virus has attacked your computer, they could be signs of a viral attack:

- unexpected error messages,
- your Macintosh "crashes" inexplicably,
- your hard disks or floppy disks are being read for no reason,
- your system seems to be running unusually slowly,
- your disk space seems to have reduced significantly, even though you have not added many files.

If your computer starts showing any of the above symptoms, there are several things you can do to check if the problem comes from a virus or from other software problems.

First, you should run Apple's Disk First Aid program. This program is designed to diagnose problems with your computer's hard disk, and repair most of them. It is installed by default in the Utilities folder of your hard disk. If Disk First Aid finds problems that it cannot repair, you will need a commercial disk maintenance program.

If this does not solve your problem, you should think about any recently installed software. Most problems with computers come from software conflicts. If you have recently installed any new software, whether applications, extensions or control panels, try uninstalling the software, and see if the problem persists.

You can restart your computer with its extensions deactivated by holding down the Shift key during startup. If you do this, your computer will start up with no extensions or control panels activated. This is another way to narrow down your problem.

You can also try using the Extensions Manager control panel to activate

and deactivate extensions and control panels. Open the Extensions Manager, which is in the Control Panel folder, and select the "Mac OS 9.0 All" set of extensions (or the equivalent for the Mac OS version you are using). This will load only original Apple extensions, and no third party software.

Your problem may come from other hardware, such as external drives, any USB hardware you may have connected to your computer, your printer driver, etc. Again, see if the problem continues when these devices and their drivers are deactivated.

For more help, you can go to the Support section of the Apple web site (www.apple.com) to see if there is a solution for your problem.

As a last resort, if you think that you have an infected file, you can send a copy of the file to the Intego Virus Monitoring Center. For information on this, see chapter 8, Technical Support.

## Basic Precautions

Even though VirusBarrier is now keeping a close eye on your Macintosh, you should still get into the habit of respecting a few basic principles to make sure that your files will always be protected.

- Make regular backups of your files.
- Make several copies of your most important files.
- When your floppy disks, or other removable media, "travel" to other computers, or if you lend them to other people, make sure they are write-protected by sliding the write-protection tabs (if possible).
- Do not deactivate VirusBarrier unless you absolutely must: you do not need to deactivate VirusBarrier to install new applications, even though most installation programs request this.
- Do not use pirated software: not only is it against the law, but these programs often carry viruses, because they travel from one

computer to another.

- With this in mind, only install programs if you are sure that the original packaging has not been tampered with.
- Think about using NetUpdate to verify that your version of VirusBarrier is up-to-date, and do this regularly, to make sure you have the latest version.
- To ensure that there is no incompatibility, only use VirusBarrier to protect your computer against viruses.

# 8 - Technical Support

Technical support is available for registered purchasers of VirusBarrier.

**By e-mail**
support@intego.com

**From the Intego web site**
www.intego.com

To send files to the Intego Virus Monitoring Center, send a copy of a file that you think is infected to support@intego.com. We will examine this file and tell you if it contains a virus, and, if it is a new virus, we will develop a vaccine for it immediately.

# 9 - Appendix

# Glossary

**Antivirus -** An antivirus is a program that protects your computer from viruses by scanning, disinfecting and repairing infected files. It looks for bits of code that make up the virus's "signature" in certain places in files and applications.

**Archive -** An archive contains several files compressed to save space.

**Boot -** Booting a computer means starting it up. It comes from the word bootstrap, as in "pulling yourself up by your bootstraps".

**Code -** Computer programs are written in code, or programming languages. Viruses, since they too are computer programs, are also written in code.

**Control Panel -** Control panels, like extensions, are part of the Macintosh operating system. They are either small programs used to add functions to the basic system, which get loaded along with the system when you boot your computer, or simple applications used to configure specific functions. VirusBarrier is a control panel.

**Desktop File -** Desktop files are invisible files that keep track of which icons go with which types of files and applications. Every volume, or disk, on your computer has invisible desktop files, called, under MacOS 9, Desktop DB and Desktop DF. Certain old viruses target desktop files, since your computer automatically reads these files whenever you insert any removable media into a drive.

**Extension -** Extensions (also called inits), like control panels, are part of the Macintosh operating system. They add functions to the basic system, or are used as drivers for specific hardware. There are two types of extensions: those that get loaded along with the system when you boot your computer, and those that are called upon when needed by the system.

**Infect -** If a file is infected, this means that a virus has copied itself into the file. This may be a macro, copied onto a word processor file, or other types of code, copied into an application.

**Hoax -** A hoax is a virus warning that is not true. There are many hoaxes that circulate by e-mail, and they all talk of getting a virus by merely reading an e-mail message.

**INIT -** An init is another name for an extension. This term comes from the fact that these files are initialized when the computer boots.

**Macro -** A macro is a short program that uses the built-in functions of an application's macro language. Many applications have macro functions, so you can carry out repetitive functions more easily. Unfortunately, viruses can be written within macros, and there are many macro viruses in the wild, especially those that run under Microsoft Word or Excel.

**Macro Command -** A macro command is a programming command that can be run in a macro. It uses a macro language specific to a given application.

**Macro Virus -** A macro virus is a virus that takes advantage of an application's built-in macro language. Macro viruses are currently the most dangerous viruses for Macintosh users, especially those that run under Microsoft Word or Excel, since they can be transmitted from Macintosh computers to Windows computers.

**Partition -** A partition, or volume, is a logical part of a hard disk. It is possible to create many partitions on a hard disk, each of which functions as if it were a smaller hard drive. The operating system sees partitions as separate volumes.

**Resource -** Macintosh files have two parts: a resource fork and a data fork. The resource fork can contain such elements as icons, code, or other instructions for applications. Some viruses hide in resources, or corrupt or change resources.

**Removable Media -** Any data storage medium that is inserted into a drive, such as a CD-ROM, a Zip cartridge, or a floppy disk.

**Strain -** A strain is a variation or mutation of a virus. Just as this term is used in medicine, for mutations of bio-viruses, it is also used for computer viruses, which can, in some cases, mutate, creating new strains.

**Trojan Horse -** A Trojan horse, or Trojan, for short, is a program which, in reality, hides some sort of malicious code. It is not really a virus, since it does not reproduce, but it may contain viral code, which, when the Trojan is run, will copy itself into other files. The name Trojan Horse comes from the huge, hollow wooden horse that the Greeks built and gave to the Trojans, apparently as a gift. The horse was taken inside their stronghold, and, later that night, Greek warriors emerged from the horse, opened the city gates, and Greek soldiers from outside stormed the city.

**Virus -** A virus is a computer program, or a bit of computer code, capable of reproducing and propagating. Most viruses are malicious, and infect files by attaching to them. They then use these host files to spread when the files are open or run.

**Volume -** A volume is a hard drive or other removable media unit. It can be an entire hard disk, a partition on a hard disk, a remote network computer, or a floppy disk. What is special about a volume is that it contains its own directory files indicating where files are stored on the volume.

**Worm -** A worm is a program that propagates itself over a network, reproducing itself as it goes. Most people think of worms as a kind of virus, since worms can be capable of malicious activities, but they do not function the same way. Worms do not need host files to reproduce.

# Virus Encyclopedia

## ANTI

The ANTI virus originated in France, in 1989. The first strain discovered was called ANTI-A, and a second strain, ANTI-B, was discovered in 1990. This virus infected applications, but not the System or data files. It is only effective under System 6.

The ANTI virus, whose name comes from the text string "ANTI" found in the virus, was a relatively dangerous virus, since it damaged applications, causing them to crash. Applications damaged by the ANTI virus cannot be repaired, and must therefore be reinstalled. This damage seems to have been accidental, however, since the virus only tries to reproduce, and has no other effects.

It seems that the ANTI-B strain was probably written before the ANTI-A strain, since ANTI-A contains code that neutralizes ANTI-B. Other than this, there is little difference between the two strains.

## AUTOSTART Worms

In May 1998, the first worm infecting Macintosh computers was found. It spread quickly through south-eastern Asia, and then throughout the world. There are several variants of this worm: AutoStart 9805-A, B, C, D, E and F.

This worm spreads easily through Macintosh computers with QuickTime's "CD-ROM AutoPlay" function enabled, if an infected CD-ROM is read by the computer. It copies itself to the host computer, creating invisible files in the Extensions folder, called Desktop Print Spooler, Desktop Printer Spooler, or DELDesktop Print Spooler.

This worm can cause serious damage to your computer, by deleting files

and destroying data. The different strains target different types of files, and corrupted files are overwritten with garbage data, and cannot be repaired or recovered. Infected computers show a great deal of unusual disk activity every 3, 6, 10 or 30 minutes, and may show Desktop Print Spooler in the Applications menu.

## CDEF

The CDEF virus was first found in 1990, in Ithaca, New York. The author of this virus, who also wrote the MDEF virus, was arrested shortly after it was discovered. Its name comes from the fact that it uses a CDEF resource, found in the Macintosh Desktop file, to reproduce. CDEF resources are normally found in certain applications, as well as in the System file, so the presence of this resource does not mean that a file is infected. This resource is not, however, normally found in Desktop files.

This virus only infected Desktop files, and could spread very easily from disk to disk, since the Macintosh reads the Desktop files of every disk when mounted. The virus did not do any intentional damage, but, like many other viruses, could still be dangerous.

A second version of the CDEF virus was found in 1993, and this new strain had only minor differences with the original.

## CODE 1

CODE 1 was first discovered in the United States in 1993. This virus was not highly destructive, and infected the System file and applications. It renamed the startup volume "Trent Saburo" if the computer was started up on any October 31. While it could spread to other computers, the only damage it could cause was crashes of the System and of certain applications.

## CODE 252

The CODE 252 virus was first discovered in the United States in 1992. It infected both the System file and applications, and would display the following message on an infected computer started up between June 6 and December 31:

> You have a virus.
> Ha Ha Ha Ha Ha Ha Ha
> Now erasing all disks...
> Ha Ha Ha Ha Ha Ha Ha
> P.S. Have a nice day
> Ha Ha Ha Ha Ha Ha Ha
> (Click to continue...)

In spite of this message, the virus did not delete any files. At any other time of the year (before June 6), the virus would merely copy itself from applications to the System file, and then from there to other applications. Crashes and corrupted files were seen under System 7, but under this system version, it would not spread to any other applications. This poorly-written virus would, however, cause other crashes and damage, since its code contains several errors.

## CODE 9811

The CODE 9811 virus was discovered in November 1998 in Sweden. It hides applications and replaces them with garbage files with names containing random letters. On Mondays, the virus has a 25% probability of displaying a message, "You have been hacked by the Praetorians," and makes the infected computer's desktop look like electric worms. This virus also attempts to delete any antivirus software on the startup volume.

## CODE 32767

This rare virus, that may no longer be in circulation, was discovered in 1997, and attempts to delete documents once a month.

## Flag

The Flag virus (also called the WDEF-C virus) infects the System file, and, while not seeking to do any major damage, overwrites the WDEF resource with ID 0. This action may cause damage. This virus may no longer be in circulation.

## Frankie

The Frankie virus, which comes from Germany, is a rare virus that only attacks certain Macintosh emulators running on Atari or Amiga computers. It seems to target pirated emulator software, and displays a message, "Frankie says: No more piracy!" and causes the Atari to crash. It does not affect Macintosh computers, but infects applications, and copies of infected applications may cause this virus to spread to other copies of the emulator.

## Graphics Accelerator

See SevenDust.

## INIT-M

The INIT-M virus was first discovered in the United States in 1993. It is a very dangerous virus, and is set to trigger on any Friday the 13th. It can corrupt large numbers of folders and files, changing their names to random strings of characters. It also changes file creators and types to random 4

character strings, which changes the files' icons, rendering them unusable, unless this information is changed back to the original. It resets the files' creation and modification dates to January 1, 1904. In some cases, the virus deletes files, and can also cause erratic window display.

This virus can infect all types of files, and also creates a file called "FSV Prefs" in the Preferences folder.

## INIT 17

INIT 17 was first discovered in Canada in 1993. It infects the System file and applications. When infected computers were started up after 6:06:06 am, on October 31, 1993, this virus would display the message, "From the depths of Cyberspace". This message was only displayed once.

It contained many errors, and could cause crashes on some 68000 Macintosh computers. This damage was more accidental than intentional.

## INIT 29

This virus was first discovered in 1988, and a second strain was found in 1994. They are sometimes called INIT 29 A and INIT 29 B respectively.

This is an extremely dangerous virus, that infects system files, applications and documents, although infected documents cannot infect other files.

While this virus does no intentional damage, other than trying to spread, it will display the following message if you insert a locked floppy disk into your computer:

The disk "xxxx" needs minor repairs.
Do you want to repair it?

In addition, various types of problems have been seen on infected computers, including crashes, miscellaneous errors and printing problems.

## INIT 1984

The INIT 1984 virus was discovered in 1992 in the Netherlands and the United States. Like many other viruses, it triggers if an infected computer is started up on a Friday the 13th. Like the INIT-M virus, it can corrupt large numbers of folders and files, changing their names to random strings of characters. It also changes file creators and types to random 4 character strings, which changes the files' icons, rendering them unusable, unless this information is changed back to the original. It resets the files' creation and modification dates to January 1, 1904.

This virus only infects INITs (or extensions), and does not infect any other type of file. It does not spread as rapidly as other viruses that affect applications, since INITs are not passed around from one computer to another very often.

## INIT 9403

This virus, also called the SysX virus, was first seen in Italy in 1994. It currently only affects Macintoshes running an Italian version of the System software. It is very dangerous, deleting files and attempting to erase currently-mounted disks. It seems that this virus was spread through pirated software, and infects the Finder, as well as certain compacting and archiving programs.

## Macro Viruses

Macro viruses pose the greatest threat for Macintosh users today.

The first real macro virus that was found in the wild was the Concept virus,

which attacked Microsoft Word files. This was quickly followed by other variants, as virus writers saw the potential to do great damage through the ubiquity of this program. Later, macro viruses were written to exploit Microsoft Excel as well. In just 5 years, since the appearance of this first virus, several thousand macro viruses have been found.

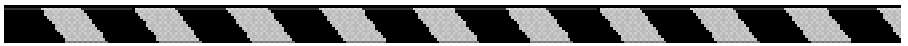
The real danger of macro viruses is the fact that they are the first cross-platform viruses. For years, Macintosh users could feel relatively secure concerning viruses, knowing that only a few dozen viruses targeted Macintosh computers, compared to thousands for Windows. But, now that macro viruses are prevalent, the danger is more present.

Most macro viruses that target Microsoft Word files use commands such as AutoOpen, AutoClose, AutoExec and AutoExit. These are commands that are executed when a certain event occurs to the file, and these four events are those which always occur when you work with a file. If, for example, a macro were written to copy itself only when you choose a certain menu command, it would be far less certain of spreading.

The most common action for macro viruses is to act when a file opens, and, first, copy themselves into the template that is opened as well. You don't physically open this template, but it is always open in the background-it contains certain customization information, such as toolbars, as well as any legitimate macros you may have added to it.

The most common macro virus that affects Microsoft Word copies itself into the active template, changes some menu items so you cannot edit the template, changes file types (which changes their icons, making them look like templates themselves), then copies itself from the corrupted template into all new files you create or open. This virus can be removed, if caught in time, by removing the active template file and any infected files.

Other macro viruses can be much more dangerous. They can corrupt or delete your files, hide certain application functions, and even more. And, on top of all that, they are cross-platform viruses, which can do damage both to Macintosh computers and PCs running Windows.



## MacMag

The MacMag virus is an example of good intentions gone wrong. It was written for the MacMag magazine, and was designed to display a message of peace, when an infected computer was started up on March 2, 1988, and then delete itself. It was originally in a HyperCard stack called New Apple Products (which, itself, was therefore a Trojan horse), and spread by infecting the System file. It is probably not in circulation any more, but may be found on old disks and CD-ROMs.

## MBDF

This virus was first discovered in Wales, in 1992, thanks to the internal virus-checking function of Claris applications. It was originally transmitted in games called 10 Tile Puzzle and Obnoxious Tetris, and a Trojan horse called Tetricycle. Unlike most viruses, the MBDF virus led to the arrest and conviction of two American college students.

The virus infects both applications and the System file, by copying an MBDF resource with ID 0. If, however, the System file already has a resource with this name, it will not be changed.

While this virus is not malicious, it can damage the System file, causing the user to have to reinstall it. It also causes certain menu-related problems. Two strains of this virus exist, MBDF A and MBDF B, which are essentially the same.

## MDEF

Four strains of the MDEF virus exist: A, B, C, and D. The A strain is sometimes called the Garfield virus, and the B strain is also called the Top Cat virus. They were discovered in 1990 and 1991 in Ithaca, New York.

The author of this virus, who also wrote the CDEF virus, was arrested shortly after it was discovered.

Its name comes from the fact that it uses an MDEF resource to reproduce. MDEF resources are normally found in certain applications, as well as in the System file, so the presence of this resource does not mean that a file is infected.

This virus attacks both applications and the System file, and can also infect documents and Desktop files. While it was not written to cause any intentional damage, it can be harmful. Some applications and other files may be damaged.

### MDEF 666

See SevenDust.

### MDEF 9806

See SevenDust.

### nVIR

The nVIR virus was first discovered in 1987 in Europe, and there are two main strains, nVIR A and nVIR B. This virus also is known under several other names, such as AIDS, Fuck, Hpat, Jude, MEV#, and nFlu.

This virus does not cause intentional damage, and reproduces by infecting the System file and applications. It will either beep, or, if MacinTalk is installed, have the computer say "Don't panic". These events occur with varying probability when the computer is started up.

### Scores

Scores, also known as the Eric, Vult, NASA and San Jose Flu virus, was first seen in 1988 in the United States. Apparently, its author wrote this virus to study virus behavior, but it quickly spread. It creates two invisible files, named Scores and Desktop_, infects the System file, and corrupts the NotePad and Scrapbook files by changing their icons. It then spreads to other applications you run, but not all applications can be infected by it. It can also cause random crashes and printing problems.

### SevenDust

There are several strains of the SevenDust virus, called A through G, and this virus is also known as MDEF 9806 and MDEF 666. These viruses spread through MDEF, MENU or WIND resources, and an extension. SevenDust E, also known as Graphics Accelerator, originated in a Trojan horse in 1998.

This family of viruses can infect applications, the System file and control panels. They attempt to delete all files which are not applications on the startup volume when the computer is running between 6 and 7 am on the 6th and 12th day of any month.

The SevenDust F strain was spread through a Trojan horse called ExtensionConflict, and this strain has five sub-strains that spread through other extensions.

### SysX

See INIT 9403.

## T4

The T4 virus was first discovered in 1992. It was part of the game GoMoku, versions 2.0 and 2.1, which was uploaded to several ftp sites. It infects applications and the Finder, and attempts to alter the System file. It also masquerades as the freeware antivirus program Disinfectant, in order to fool other antivirus programs.

It can cause irreparable damage to the System file and random crashes. It can also prevent your computer from booting.

Another strain, T4-D, was found in 1997. This deletes files and documents in the System folder, but not the System file. It spreads from one application to another, by attaching itself to the application's CODE resource.

## WDEF

The WDEF virus, first found in Belgium in 1989, gets its name from the WDEF resource found in the Desktop file. Its two strains, WDEF A and B, spread by infecting these files, and, since the System reads the Desktop files of every disk it mounts, can spread very easily, without even needing applications to run.

It does not do any intentional damage, but some of its programming errors can cause problems, such as crashes, and font display problems.

## ZUC

The ZUC virus was first found in 1990, and is named after its discoverer, Don Ernesto Zucchini. There are three strains of this virus, ZUC A, B and C. They infect applications only, and can spread even if the applications are not run. They cause erratic cursor behavior, but do no other damage.