InoculateIT®

Personal Edition
For Windows 95, 98 & NT

Getting Started

Version 5.1

COMPUTER ASSOCIATES®
Software superior by design.

Welcome to InoculateIT Personal Edition

Congratulations on choosing InoculateIT Personal Edition (InoculateIT PE) to protect your computer against viruses, trojans, backdoors and other malicious software. InoculateIT PE is a high performance virus package specifically designed to protect small businesses and home users from everyday virus threats.

InoculateIT PE protects individual computers without having to be installed from a network server. If you wish to install anti-virus protection to several computers in a business environment, we recommend that you evaluate other InoculateIT anti-virus products.

InoculateIT PE includes FREE software updates to registered users. In addition, if you find a virus that InoculateIT PE is unable to detect or clean, we attempt to send an emergency signature update in approximately 48 hours of receiving a copy of the suspected infected file.

Registered users will also receive FREE Internet E-mail support. The answers to many support questions may also be found in the online help. Simply open InoculateIT PE then select Help | Help Topics, then select "How to get Technical Support and FAQs" you will find the answers to most of the questions that are generally asked of our support team.

When you register your software, you are automatically subscribed to our FREE Virus Threat Notification System as well as our Update Notification Service. Anytime a new virus is found that is actually spreading around the world, this service will send an e-mail to you when a new virus signature update is available. This handy service will ensure that you are kept up to date so that you are protected against the very latest viruses.

Note: The Update Notification Service will only alert you when a new virus signature is posted on the Internet.

Installing InoculateIT PE

Before installing InoculateIT PE, please close all other Windows programs as they may interfere with the installation process. If you already have another anti-virus product loaded you MUST disable its Real-Time Protection (background checking) before installing InoculateIT PE.

If you are installing InoculateIT PE for the first time you need to make a boot disk and a reference disk.

Windows 95/98 Boot Disk:

1. Select Start | Run...
2. Type FORMAT A: /S and press <Enter>
3. Put a blank disk in drive A: and press <Enter>.
4. When the disk is finished, take it out and label it 'Boot Disk'. This disk can be used to start your computer if your Windows 95/98 operating system becomes corrupt.

The reference disk will be created during installation.

Windows NT Boot Disk:

1. On a Windows 3.1x, 95 or 98 PC, put a blank disk into drive A:.
2. Type FORMAT A: /S and press <Enter>.
3. When the disk is finished, take it out and label it 'Boot Disk'. This disk can be used to start your computer if your Windows NT operating system becomes corrupt.

The reference disk will be created during installation.

If you are upgrading your InoculateIT PE software, we recommend that you take the time to read the README.HLP file that is in your InoculateIT PE directory. If you only wish to update the list of viruses that InoculateIT PE can detect then please see “DAT File Updates” in this chapter.

Important! You MUST login as an Administrator to install InoculateIT for Windows NT.

How to Install InoculateIT PE

1. Go to http://antivirus.cai.com and select "Download Free Anti-Virus Software".

   If you registered previously, you are taken directly to the download page otherwise you will have to register.

2. If prompted for registration, fill out the registration form and press the Submit button.

3. View the legal agreement and accept it by pressing the "I AGREE" button. This takes you to the download page where you follow the instructions to download InoculateIT PE.

4. Run the file that you have downloaded.

   The InoculateIT PE splash screen will appear.

5. Click the Next> button to move on to the Welcome screen.

   This reminds you to stop any other programs while installing InoculateIT PE. For example, if you are running a telecommunications program, or a game, we recommend that you stop that program before continuing.

6. If you have no other programs running, click Next> to proceed.

7. Setup will display the InoculateIT PE licence agreement. The licence conditions must be accepted for the installation to proceed. Click Yes to proceed.

8. The Setup Options dialog displays and you can select from Typical or Custom setup.

   The "Typical" installation has default settings and is simpler to install. The "Custom" installation allows you to configure each option.

Typical Installation

Setup will display the Check Setup Information dialog. This allows you to confirm the directory that InoculateIT PE will be installed to.

1. Click Next> to accept the default and the files will be copied to the directory.

   Follow the instructions of Installation Wizard. Select the Help button for further information on any option

   Once you have completed installation of this latest version of InoculateIT PE it will be able to detect many more viruses. Therefore, we recommend that you accept this option and run a full scan after installation.

DAT File Updates

Due to the large number of new Viruses that keep appearing it is necessary to install new DAT files into the anti-virus engine to keep it up to date. Update files will be able to detect and clean all of the latest viruses.

The easiest way to update the DAT files is to open InoculateIT PE and select Tools | Auto Download, then follow the on-screen messages.

1. Open Netscape or Internet Explorer and go to http://www.cai.com/antivirus/ personal.

2. Select “Download Free Software Updates”, then “IPEup320.exe” and “Save this program to disk”. (note that the number (320) in this name will change as newer versions are released). Copy this file onto the machine you wish to update.
3. Once the file has been copied to the machine that you wish to update, double click on the file to run it, then follow the on screen messages.
4. Once the update has been installed, the update file will be copied to your InoculateIT directory. If you wish to update your resident protection you need to reboot your PC. Once it has been rebooted InoculateIT PE will be able to automatically find all of the latest viruses.

Cleaning Viruses with InoculateIT PE

InoculateIT PE has two methods of scanning for viruses. The first is done in the background while you are performing normal tasks on your PC. The other is when you actually start InoculateIT PE and scan selected files and drives. The following sections outline the recommended default settings for background scanning and the recommended method for removing viruses when they have been detected.

How to Remove Viruses in Memory

Virus Detected in Memory While Running a InoculateIT PE Scan

Provided the Memory tab on the Options | Program menu has **Enable Memory Scanning** selected, InoculateIT PE will detect and if possible disable viruses in memory as part of the first scan performed in any session.

When a virus has been detected, a dialog appears with the name of the virus and allows you the option of disabling it. Select Yes and a message confirms that InoculateIT PE has disabled the virus(es). Once the virus is removed it is recommended that you scan all hard drives and any floppy disks that may be suspect.

Virus Detected in a File While Running Windows

Provided the Enable File Monitor Real-Time Protection option is selected on the Options | Real-Time Protection menu, InoculateIT PE monitors selected file activities such as opening, closing, copying and running. See the Options | Real- Time Protection menu or the on-line help for details about the activities that can trigger scanning.

How to Remove Boot Sector Viruses

InoculateIT PE's automatic floppy scanner will detect boot sector viruses when Windows attempts to reference a floppy disk. Hard drive boot sectors can only be scanned from InoculateIT PE.

Floppy Disk Boot Sectors

By default, Real-Time protection is installed to detect boot sector viruses automatically, to replace the infected boot sector with a standard floppy boot sector, and to report the name of the virus, in a dialog, to the desktop. The defaults can be modified through the Options | Real-Time Protection menu. The on-demand scanner can also detect and repair infected floppy disk boot sectors.

The settings for this are controlled by the Options | Program | Boot Sector tab. If an infected floppy is scanned (and it is not write protected) the boot sector will be automatically replaced and a dialog will display the name of the virus that was removed.

Hard Disk Boot Sectors

When InoculateIT PE detects a boot sector virus on the hard drive the Repair Infected Boot Sector dialog displays.

1. The name of the drive and the type of virus found will be displayed and InoculateIT PE will ask if you would like the virus removed. The options are:

   Yes - create a rescue disk before removing the virus

   No - do nothing except report the virus to the log file

   Details - gives information about the infection

   Help - displays the appropriate On-line help screen

2. If Yes is selected the Make A Rescue Disk dialog displays. This creates a snap-shot of the current system which can be used to re-install the current boot sector in case the removal of the virus corrupts the disk. It is strongly recommended that a rescue disk be created.

   Next, InoculateIT PE checks to see if the boot sector can be recovered from the virus. The help button displays the appropriate on-line help screen.

3. If Yes is selected InoculateIT PE attempts to remove the virus. If the virus has not corrupted the original boot sector, it will be located and re-instated. If the original boot sector is unrecoverable InoculateIT PE will offer to install a standard boot sector. This standard boot sector is successful for the vast majority of PCs.

Once the InoculateIT PE application has been started, the defaults for any boot sector scans are determined by the Options | Program | Boot Sector tab. See the On-line help for more information on each of these options.

How to Remove File Viruses

File viruses will be removed automatically if the Options | Program | Action tab has been set to Clean Infected Files. Other possible options are to delete or rename the file. Whichever option is selected, the name of the virus and the name of the infected files will be written to the log file.

When a scan is performed on a group of files, the file name of the infected file(s), the name of the virus, and the action InoculateIT PE has taken, will be displayed in the InoculateIT PE Report window. By default only those files that are infected will be displayed. All the files scanned can be displayed if the InoculateIT PE Options | Program | Reporting tab All Files Scanned option is selected.

Cleaning Macro Viruses

The term "macro virus" is used to refer to any virus written in a program's macro language. The danger with these macro viruses is that, although they are contained in Word documents, Excel spreadsheets, PowerPoint presentation, Access databases and other Microsoft applications, they are also executable code. Thus, the simple act of opening a document or spreadsheet can allow a macro virus to activate - and infect your system.

When a scan is run on a file, directory, or drive, InoculateIT PE will automatically clean Microsoft Word and Excel macro viruses provided the Options | Real-Time Protection | Enabling | Enable Real-Time file monitor is selected.

If the document has been infected with a mutation of an existing virus, only the macros that are known to exist in other viruses will be deleted. This is normally sufficient to permanently disable the virus.

Getting Help

We provide a comprehensive online help system to assist you in using InnoculateIT PE and enable you to exploit the full functionality and unique features of the software.

If you have a technical support question, the Frequently Asked Questions (FAQ) section of the help may provideimmediate answers to your questions. For further technical assistance with this product, you may also contact Computer Associates InoculateIT Personal Edition technical support staff 24 hours a day, 7 days a week at IPE_Support@cai.com.