

## **Best Practices for running anti-virus : (will be updated from time to time)**

To reduce the risk of virus infections, and reduce the possibility of inadvertently triggering or spreading viruses to other people, you should be aware of some easily implemented "safe computing" practices. Put these into effect on your machine today and they will help make your system less prone to malicious code attacks.

**PLS NOTE: IN A SCENARIO, WHERE A CLIENT IS MAJORLY INFECTED AND YOU FEEL THAT ONE SOLUTION IS NOT PROVING ENOUGH, YOU CAN USE THE HOUSECALL FREE SERVICE FROM ANY ANTIVIRUS SOLUTION PROVIDER I.E NORTON/MCAFFEE AND SCAN THE CLIENT. PLEASE REMEMBER ONLY THE HOUSECALL FEATURE AND NOT THE ANTI-VIRUS SOFTWARE, THE REASON FOR NOT USING THE LATTER IS EXPLAINED BELOW.**

### **This one is focused on the software solution from Trend Micro.**

#### **Damage Clean Server: (mandatory)**

Prior to installation of the anti-virus software, run a housecall on your client. This will clean up any existing virus/worms from your client. Subsequently, the software that will be installed, will ensure sustained protection.

#### **Trend's OfficeScan Anti-Virus Protection Software**

Installing Trend's OfficeScan on Workstations connected to your Network.

#### **Instructions for installation:**

Note: For Windows NT/2000 Local Administrator privileges are needed to install OfficeScan on a computer.

1. **Uninstall any existing antivirus software** - most antivirus products view other antivirus products as virus-like activity. If needed, check the antivirus vendor website for the latest uninstall software.
2. **Close any unnecessary programs you may be running** - as with most software installations, best practice dictates closing all programs that are currently running.

4. On the startup page, click the **Install Now** button. A permission to install page will appear in the center of your browser. Click the "**yes**" button. Three more confirmation pages will appear. Click "**yes**" on each one of them.
5. A progress page will appear showing the download and install status. When the install is complete a page will open signifying the completion of the installation. Click **OK** and close Internet Explorer.
6. You will notice a new icon in your system tray (box including the time in lower right corner of the screen). This **blue computer icon** signifies that OfficeScan is loaded on your computer.
7. To scan your own computer, right click on icon and select **OfficeScan main**. A menu will open allowing you to select areas to scan. Initially, select the hard drive, C, and press the large **Scan Drives** button. Note: This will take a few minutes; so you may want to perform the hard drive scan during a lunch period. Use the OfficeScan main option for future scanning of the floppy, zip, and CR-ROM drives. A window will appear advising you of the progress of the scan. Close the window when finished.

OfficeScan is a **load and forget** product. Once an initial scan is completed, OfficeScan will **automatically scan files** for viruses and **automatically receive virus signature updates from Trend Enterprise Antivirus Server** when the computer is connected to your network. **There is no need to connect to a remote web site and download virus signature updates**

### **Client end checks and do's:**

#### ***Procedure to be followed for Protecting the Systems from Virus Attacks***

Infected clients to be immediately disconnected from the network and cleaned for infections and application of all necessary patches for OS ,Browsers, SQL 2000 and IIS servers.

#### **Apply All the Latest Microsoft Security Updates**

In order to close security holes that have been discovered since Windows was shipped and installed, we advise everyone to visit the Microsoft Update Website at <http://windowsupdate.microsoft.com>.

Or

Please visit <http://v4.windowsupdate.microsoft.com/en/default.asp>

Please follow the on-line instructions on how to update your system. Security updates will help prevent hackers from accessing your system and prevent viruses from running on your system.

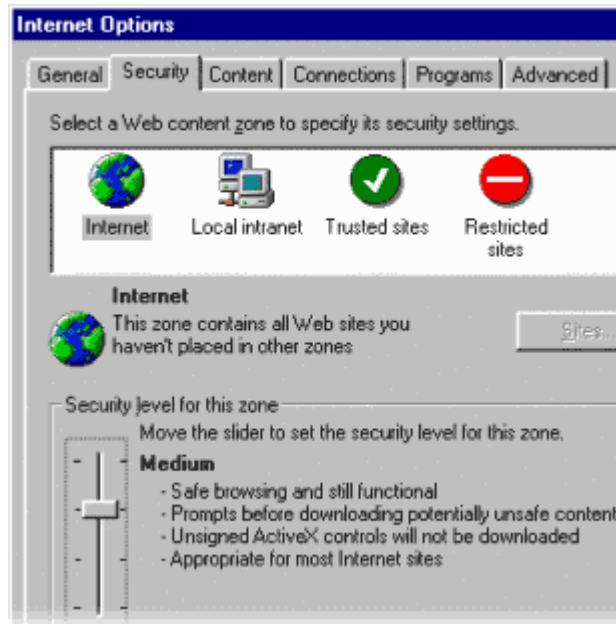
Windows 98 or Windows 2000 users can also use the Windows Update feature to get all the latest security updates.

- Use IIS Lockdown tool to secure IIS servers. (Available from <http://www.microsoft.com/downloads>)
- close port tcp/69 (tftp) service. ( services file)
- Remove all share drives and shared folders. Avoid direct disk sharing with read/write access unless there is absolutely a requirement to do so.
- Never download files from unknown or suspicious sources.
- Delete spam, chain, and other junk email without forwarding.
- Never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately then “ double delete” them by emptying your Trash
- Always scan a floppy Diskette from an unknown source for viruses before using it.
- Never use more than one anti virus software on a single client as this will result in a conflict and neither of the software will work fine.
- Never download any Free Antivirus Software/tools from un-trusted sources. They claim that they protect your computer but they make your PC vulnerable by terminating the antivirus programs and planting new viruses .
- **Internet Explorer Security to atleast "Medium"**

By default, the Internet Explorer Security Setting is set to "Medium." However, Trend has seen many systems where the security system was changed to "Low" by a virus, Trojan, or hacker.

In this regard, we encourage every user to ensure that their security setting is set to at least "Medium", as this will reduce the risk of accidentally running a malicious file.

At the "Medium" security level, Internet Explorer 5 will prompt users before running potentially unsafe content.



Internet Explorer 5 or above will also display a warning message before running any Active-X controls (as shown on the picture below).

- In a scenario, where your software is detecting the virus/worm but is unable to clean it. Take your system off the network, recheck that no unwanted service is running and then restart the scan.
- **Establish a Strong Password Policy**

Protecting systems against viruses and hackers requires the use of strong passwords. Several malicious programs attempt to connect to your system by using common passwords (such as windows, exchange, user, etc) or guessing thousands of common words found in the dictionary. It is recommended that you:

Always protect your password:

- Never share your password with anyone
- Do not write it down, especially on a sticky note next to your computer

Choose strong passwords:

- Never choose family names, birthdays, or other words commonly found in the dictionary
- Select passwords with a minimum of 8-10 characters
- Use a combination of lower and upper case letters, numbers, and non-alphanumeric symbols (like the percent (%) or dollar (\$) symbol)

### Additional Instructions for windows XP/ME

Windows Millennium Edition (ME) and Windows XP have a feature known as System Restore, which creates backups of certain files in the \_Restore folder. The System Restore feature usually backs up files with EXE or COM extensions, which may include infected files and malware programs. Files in the \_Restore folder are protected and can only be accessed using System Restore. This feature must be disabled first before Trend Micro antivirus can access and clean these files.

The following procedure disables the System Restore feature:

#### **For Windows ME**

- Right-click the My Computer icon on the Desktop and click Properties.
- Click the Performance tab.
- Click the File System button.
- Click the Troubleshooting tab.
- Select Disable System Restore.
- Click Apply > Close > Close.
- When prompted to restart, click Yes.
- Press F8 while the system restarts.
- Choose Safe Mode then hit the Enter key.
- After your system has restarted, continue with the scan/clean process. Files under the \_Restore folder can now be deleted.
- Re-enable System Restore by clearing Disable System Restore and restarting your system normally.

#### **For Windows XP**

- Log on as Administrator.
- Right-click the My Computer icon on the desktop and click Properties.
- Click the System Restore tab.
- Select Turn off System Restore.
- Click Apply > Yes > OK.
- Continue with the scan/clean process. Files under the \_Restore folder can now be deleted.
- Re-enable System Restore by clearing Turn off System Restore.

## Frequently Asked Questions

### OfficeScan

Q.1 How to manually update OfficeScan clients?

**To perform Update Now on the client:**

1. Right-click the OfficeScan icon in the system tray.  
The OfficeScan shortcut menu appears.
2. Click Update Now.  
The Update Now settings screen appears.
3. In the Domain name/IP address list, choose an update source.
  1. If the user wants to download from the OfficeScan server, verify that the domain name/FQDN or IP address of the server is correct.

*Note: If you are downloading directly from the Trend Micro ActiveUpdate server, you can only update the pattern file and scan engine.*

4. In the Server port, verify that the server port number, which the client uses to communicate with, is correct.  
The default port number is port 80, which is also used as the HTTP port.
5. If a proxy server has been set up to handle client-server communication on the network, select the Use a proxy server check box.
6. Type the proxy server address and port number in the text boxes. If the proxy server requires a user name and a password, type user name and password.
7. Click Update Now.

The client connects to the selected update source to check for updates.  
If updates are available, the client automatically downloads these.

Update now is automatically done in the background and performed on a scheduled basis

**Q.2** How to handle virus pop-ups on the client?

When the real-time service starts on a Windows NT or 2000 client workstation, OfficeScan Corporate Edition 5.0 displays a pop-window stating that the service is starting. Is there any way to hide this pop-up window?

You can disable the pop-up window by doing the following:

Run the Registry Editor (regedit.exe) and go to following folder: HKEY\_LOCAL\_MACHINE\Software\TrendMicro\PC-cillinNTCorp\Currentversion

Add the following key and value in this registry folder: ShowSplash = 0

The value "0" disables the splash screen. To enable the splash screen again, change the value to "1".

**Q.3** How to update clients behind the proxy?

Create a Mobile Remote agent package by doing the following:

1. Go to ..\PCCSRV\Admin\Utility\RA\_En or ..\PCCSRV\Admin\Utility\RemoteAgent directory.
2. Run the RAPacker.exe.
3. Select the option to **Create Mobile Agent Setup package**.
4. Click **Start** to begin.
5. Check **Get updates from Trend ActiveUpdate Server**. Make sure that it points to: <http://officescan-t.activeupdate.trendmicro.com/activeupdate>
6. If the client workstation uses a proxy server to connect to the internet, select the **Use a proxy server** option and configure the proxy settings.
7. Click **Next**.
8. Set the value for the **Interval for Checking for Updates** option. Click **Next**.
9. If you want the client to periodically check the client connection using the OSCE serverSet, select the **Schedule Verify Connection** option. Otherwise, clear this option.
10. Specify a location to create the setup packages. Click **Next**.
11. Click **Yes**.
12. Click **Done** to finish creating the packages.

After creating the package, run the RAPacker.exe file created on the remote workstation to allow getting updates directly from the Internet.

Q.4 How to reset OfficeScan server password?

Open the ofcscan.ini file in notepad/ wordpad.  
Find the string "License Key", and replace the contents of the key with "70".  
Doing this will change the OfficeScan console password to "1".

Q.5 How to move a client to another or new OfficeScan Server?

There is a tool available in pccsrv\admin\utility\ipxfer directory by the name ipXfer.exe.

Use the tool with the syntax as below: -  
IpXfer.exe -s <OSCE server IP> -p <OSCE port> -m 1 -c 12345 -v 5.5

Q.6 How to update the pattern file on the clients, in case OfficeScan Server is down?

**To allow users to download from the Trend Micro ActiveUpdate server:**

1. Open the OfficeScan Management Console.
2. On the sidebar, click Client Administration.  
The domain tree for Client Administration appears.
3. Click the domains or clients to grant Scheduled Update privileges by clicking the corresponding icons in the domain tree.  
To select all domains and clients, click the root icon.
4. On the sidebar, click Set Privileges.  
  
The Set Privileges screen appears.
5. Under Update, select the Download from the Trend Micro ActiveUpdate server check box.
6. Click Apply to grant the privilege to the selected domains or clients.

*Note: If the user clicked the root icon before setting privileges, another button named Apply to all clients will appear beside Apply. If the user wants all existing and future clients to have this set of privileges, click Apply to all clients.*

**To perform Update Now on the client:**

1. Right-click the OfficeScan icon in the system tray.  
The OfficeScan shortcut menu appears.
2. Click Update Now.  
The Update Now settings screen appears.
3. In the Domain name/IP address list, choose an update source.
4. If the user wants to download from the OfficeScan server, verify that the domain name/FQDN or IP address of the server is correct.
5. If the user wants to download from the Trend Micro ActiveUpdate server and has been granted this privilege, click the Domain Name/IP address arrow, and then click the address of the Trend Micro ActiveUpdate server.

The default address is:

[officescan-t.activeupdate.trendmicro.com/activeupdate](http://officescan-t.activeupdate.trendmicro.com/activeupdate)

*Note: If you are downloading directly from the Trend Micro ActiveUpdate server, you can only update the pattern file and scan engine.*

6. In the Server port, verify that the server port number, which the client uses to communicate with, is correct.  
The default port number is port 80, which is also used as the HTTP port.
7. If a proxy server has been set up to handle client-server communication on the network, select the Use a proxy server check box.
8. Type the proxy server address and port number in the text boxes. If the proxy server requires a user name and a password, type user name and password.
9. Click Update Now.  
The client connects to the selected update source to check for updates. If updates are available, the client automatically downloads these.

Update now is automatically done in the background and performed on a scheduled basis

Q.7 Pre-installation hardware/software requirements in order to install Anti-virus software?

### **OfficeScan™ Server (HTTP-based)**

#### Hardware Platform

- Intel™ Pentium™ III processor or equivalent
- 256MB RAM (preferred 512MB)
- 300MB disk space
- Monitor that supports 800x600 resolution at 256 colors or higher (Windows NT only)

#### Software Platform

- Windows™ 2000 Server, Windows 2000 Advanced Server, or Windows 2000 Professional (with SP2)
- Windows NT 4.0 Server/Workstation (with at least SP5)
- Microsoft Internet Explorer 5.0 or higher
- Microsoft Internet Information Server (IIS) 4.0 or higher
- If you are installing the server on a Windows NT Server, you must have Administrator or Domain Administrator privileges to the target server.
- File and Printer Sharing for Microsoft Networks must also be installed on the server

### **OfficeScan™ Client**

#### OfficeScan client for Windows Me/98/2000

#### Hardware Platform

- 133MHz Intel Pentium processor or equivalent
- 128MB of RAM
- 80MB of free disk space
- Monitor that supports 800 x 600 resolution at 256 colors or higher

You may need more RAM and disk space if you also install POP3 Mail Scan, Outlook Mail Scan, Check Point SecureClient support, and other tools.

#### Software Platform

- Windows 98/Me/2000
- Microsoft Internet Explorer 5.0 or later

#### OfficeScan client for Windows 2000/NT

#### Hardware Platform

- 150MHz Intel Pentium processor or equivalent
- 128MB of RAM
- 80MB of free disk space
- Monitor that supports 800 x 600 resolution at 256 colors or higher (Windows NT only)

You may need more RAM and disk space if you also install POP3 Mail Scan, Outlook Mail Scan, Check Point SecureClient support, and other tools.

#### Software Platform

- Windows NT 4.0 workstation (with at least SP5 installed), or Windows 2000 Professional or later
- Microsoft Internet Explorer 5.0 or later

#### OfficeScan client for Windows XP

#### Hardware Platform

- 233MHz Intel Pentium processor or equivalent
- 128MB of RAM
- 80MB of free disk space
- Monitor that supports 800 x 600 resolution at 256 colors or higher

#### Software Platform

- Microsoft Windows XP Professional or Home Edition

\* Supports Microsoft Windows XP Tablet PC Edition

#### Q.8 What is TrendMicro System Cleaner (TSC)?

TSC is a special fix-tool being created by Trend Micro in order to do a lot of tasks like; removing Trojans, removing drop-files of the Trojans/worms, cleaning up the registry settings; all those tasks which would otherwise require a human intervention (manual process).

It has been integrated with OfficeScan and ServerProtect software and can be easily downloaded from the link below: -

<http://www.trendmicro.com/download/tsc.asp>

#### Q.9 What is OfficeScan?

OfficeScan™ Corporate Edition provides comprehensive virus protection for desktop and mobile clients. OfficeScan offers centralized management features, which allow administrators to fully manage and enforce antivirus policies across the entire organization. Designed to provide reliable and transparent virus scanning and virus removal, OfficeScan incorporates robust damage cleanup services, which help remove malicious code and repair system damage caused by malicious code.

#### **Key Features**

- Centralized Management, Updating, and Reporting
- Easy Migration and Deployment
- Reliable and Comprehensive Virus Protection
- Support for Trend Micro Enterprise Protection Strategy

➤ Fast, Automatic Virus Pattern File Updates

Q.10 Deployment scenarios for OfficeScan?

OfficeScan can adopt several client deployment methods. A part of deployment planning involves selecting preferred client installation method(s). For step-by-step instruction on how to implement each of these client deployment options, refer to the OfficeScan Quick Installation/Migration Guide.

- Login scripts – adding an OfficeScan client installation/update program, AUTOPCC.EXE to the login script will ensure all users are installed and updated with the latest client program and Pattern/Engine files. Whether the server was installed as HTTP-based or file-based server, this is the most automated and sure way of deploying OfficeScan antivirus agents to all desktop computers. When users log into a server with login script that contains a command line to AUTOPCC.EXE program on the OfficeScan server, the program will install OfficeScan to the user's desktop computer. If OfficeScan is already installed, AUTOPCC.EXE program will update the OfficeScan if any new updates become available.

- Web Install – using Internet Explorer Browser 4.0 or above, users can connect to the OfficeScan server and initiate installation right from their browsers. (Available only from HTTP-based server)

On the other hand, the administrator may send out email to all employees, with a URL link to the installation page on the OfficeScan server, and ask them to click on the link and install OfficeScan antivirus agent to their desktops.

- Remote Installation (for Windows NT) – The administrator, with appropriate access privileges to the remote NT workstations, may remotely install OfficeScan antivirus agents to the said NT workstations on the network. (Available only to NT clients).

The administrator may install on one or multiple NT workstations at once. If all NT workstations share the same domain or administrator account and password, access credentials need only be entered once.

- CD-ROM-based Installation – OfficeScan client setup programs can be copied to a CD-ROM, where the user can install from. The installed client will report to the server where the client setup program was retrieved from. This is useful if the target client machine does not have a fast network connection to the server or if the clients are remote and rarely connect back to the server.
- Distribution Shares – to distribute the load of installation, administrator may distribute server loads to other servers other than the OfficeScan server. Copying the OfficeScan directory, \PCCSRV\, from the OfficeScan server to any other file servers, and direct end users to install from the file server, does this. After installation, the OfficeScan agent will still report to the original OfficeScan server to get updates and configurations.

Q.11 Database restoration of OfficeScan server in case the database gets corrupted?

### **On the OfficeScan server**

Note: Use an administrative account before proceeding. If not, logoff and logon again as an administrator of the OfficeScan server.

1. Stop the following services in Windows Control Panel Service's list
  - OfficeScan Master Service
  - World Wide Web Publishing Service
2. Remove the "Everyone" group or any other account which has access to the OfficeScan shared home directory (..\PCCSRV)so that no client will be able to access the OfficeScan server during the restoration of the database.
3. Replace the files located in the ..\PCCSRV\Database folder with the backed up database.
4. Check the security permission of the ..\PCCSRV\Database folder and make sure that the "Everyone" group has at least change permission on that directory and its subdirectories. Be sure to select the "Replace permissions on subdirectories" and "Replace permissions on existing files" checkboxes and then click "Apply" button.
5. Bring back the "Everyone" group or any other account that was removed earlier in the permission of the OfficeScan Home directory so that they will have access again to the OfficeScan server.

### **On the OfficeScan client workstation**

Logoff and logon again on the network again to be able to use the new database.

Q.12 How to enable PoP3 scanning of emails using OfficeScan clients?

**The files that are needed are the following:**

Mainfile:pop3pack.exe

Related files : pop3trap.exe, pop3unis.exe, pop3util.dll, pew952.dll, pewnt2.dll, tmdbg.dll,pc-cillin.ini

### **Usage**

Do the following:

### **On the OfficeScan client workstation;**

1. Go to the ..\PCCSRV directory of the OfficeScan server and copy pop3pack.exe.
2. Double-click pop3pack.exe to install POP3 Scanner on the OfficeScan client.

Six files will be extracted to the OfficeScan client folder (i.e. pop3trap.exe,

pop3unis.exe, pop3util.dll, pew952.dll, pwent2.dll, tmdbg.dll and pc-cillin.ini), and pop3trap.exe will be automatically launched as soon as the extraction is completed.

3. Open the client's email client and check if the account settings have been modified. The incoming server should have already been changed to localhost and the account name should now be name/pop3server, where "name" is your account name and "pop3server" is your POP3 mail server.

*Note: If the settings are the same as before you extracted pop3pack.exe, this indicates that pop3pack.exe is not running because it was not correctly installed. Restart the mail client in order for the changes to take effect if necessary.*

4. The settings of the POP3 scanner are the same as the Real Time Scan configuration of the OfficeScan client on the machine, therefore the POP3 scanner can be set from the OfficeScan Management Console > Real Time Scan settings or on the Real Time Scan settings of the Client Console. The default scan action for POP3 Scanner is AutoClean, then DELETE if uncleanable. Note that the Rename and Quarantine actions do not work with POP3 Scanner. If POP3 Scanner is configured to Rename or Quarantine infected files, it will Delete these files.

*Note/s:*

*1. POP3 Scanner can scan compressed attachments that have a maximum decompressed file size up to 30 MB. Any attachment with a file size more than 30 MB when decompressed may not be retrieved and may result in a time-out.*

*2. POP3 Scanner cannot delete an uncleanable infected file inside a compressed file, even if you have set OfficeScan to delete uncleanable files. The uncleanable file will be passed instead. To unload POP3 Scanner, run pop3unis.exe, which either located in the OfficeScan client folder or the Uninstall folder.*

*3. To uninstall POP3 Scanner, you must uninstall the OfficeScan client program. POP3 Scanner alone cannot be uninstalled.*

Q.13 What files needs to be backed up regularly so as to restore the server in case it gets crashed/ corrupted?

The following files should be available in the machine:

- DBBackup.exe
- Tmdbg20.dll

Create backup files by doing the following:

1. Go to the \Pccsrv\Admin\Utility\DBBackup folder.
2. Run the DBBackup.exe tool from its current directory. The DBBackup icon appears on the Windows task bar.
3. Right-click on the DBBackup icon. A pop-up menu appears with the following options:

- **Backup Now** – Select this option to immediately backup the database files.
- **DB Backup Settings** – Select this option to configure scheduled backups and to specify the source and destination folders.

Selecting this option opens the DBBackup user interface. The system displays the following fields:

- **Database path** – Enter the UNC (Universal Naming Convention) path of the databases that will be backed up.
- **Backup path** – Enter the UNC destination path of the backup database files.
- **Schedule for backup** – This option lets you specify daily, weekly, or monthly backups, or no schedule.

*Note: Use the last option if you prefer to perform the backup on demand.*

Q.14 How to restore the OfficeScan Server?

Create / restore the virtual directories in OfficeScan using the following steps:

1. Run the command prompt.
2. Type the `srvinst -setvirdir` and then press Enter key.

The virtual directories will be created under the OfficeScan directory.

These directories are as follows:

Officescan  
Officescan/hotdownload  
Officescan/download  
Officescan/cgi  
Officescan/clientinstall  
Officescan/html  
Officescan/remotestallcgi

## ServerProtect

Q.15 What is ServerProtect?

ServerProtect™ provides comprehensive antivirus scanning for servers, detecting and removing viruses from files and compressed files in real time -- before they reach the end user. Administrators can use a Windows-based console for centralized management of virus outbreaks, virus scanning, virus pattern file updates, notifications, and remote installation. ServerProtect supports Microsoft™ Windows™ Server 2003, Microsoft Windows 2000, Microsoft Windows NT™ 4, and Novell™ NetWare™ servers.

### Key Features

- Microsoft Windows Server 2003/2000 Datacenter Certified
- Reliable Virus Protection
- High-performance Scanning
- Centralized Management and Reporting
- Support for Trend Micro Enterprise Protection Strategy
- Fast, Automatic Virus Pattern File Updates
- Robust Log Reports and Notifications

Q.16 Difference between ServerProtect Information Server and Normal Server?

ServerProtect™ Information Server holds the information about all the Normal Servers reporting to it. ServerProtect IS is the central repository of the entire database of all the servers protected with ServerProtect NS software in the network.

ServerProtect™ Normal Server is the actual software code that does the protection/ scanning of incoming/ outgoing files on to the specific server hard disk. ServerProtect NS generates logs and transfers them to the ServerProtect IS reporting.

Q.17 What files needs to be backed up regularly so as to restore the server in case it gets crashed/ corrupted?

To back up Information Server(s):

1. Do one of the following:

- Right-click the server's icon in the domain browser tree and choose Backup IS Data from the pop-up menu.
- Choose Information Server | Backup IS Data from the main menu.

2. The Back Up Information Server dialog box opens. The Information Server text box shows the server that is designated as the Information Server.

3. Select the server and the shared folder that will hold the backup from the tree at the bottom of the dialog box.

4. Enter the Username and Password to log on the server that you specified in the Backup to field.

5. Specify whether you want to schedule the backup to be performed regularly from the Frequency scrolling list. Your options are: Daily, Weekly, and None. If you choose Weekly, you need to specify the Day of the week and Time for ServerProtect to perform the backup. If you choose Daily, then you only need to specify Time to perform the backup.

6. Click the Automatically backup data when the server tree or a task changes option box if you want ServerProtect to automatically backup IS data when you remotely install/uninstall a server, or when you modify a task. Doing this prevents you from losing all the information of the ServerProtect servers if the remote installation/uninstallation fails. You can retrieve your backup task definition to a newly installed server without re-configuring a new task.

7. Click the Apply button to activate this function. Or click Cancel to close the window.

OR

1. Launch ServerProtect Management Console.
2. Type the ServerProtect Administrator password.
3. In the main menu, click Information Server > Backup IS Data.
4. Stop the Trend ServerProtect Agent service in Windows Control Panel Services List.

Q.18 How to restore the ServerProtect from the backup files?

**B. On the New Information Server:**

1. Install ServerProtect for NT 5.20 Information Server.
2. Launch ServerProtect Management Console.
3. Type the ServerProtect Administrator password.
4. In the main menu, click Information Server > Restore IS Data

*Note: To verify if transfer is successful, check the ServerProtect Domain tree. The Normal Servers should be displayed in the Domain tree.*

## General Questionnaire

Q.19 What is Safe Computing and how to do it?

You can get the required information from <http://support.nic.in>

Q.20 From where can you get the latest updates/patches?

FROM NICHQ CENTRAL SERVER. In the eventuality that it is down:

- a) From the Trend Micro website (pattern file)  
<http://www.trendmicro.com/download/pattern.asp>
- b) From the Trend Micro website (scan engine)  
<http://www.trendmicro.com/download/engine.asp>
- c) From the NIC network, do contact your local administrator or write an email to [support@nic.in](mailto:support@nic.in)/[antivirus@nic.in](mailto:antivirus@nic.in)

Q.21 Whom to call in case of emergency?

Kindly, write an email to [support@nic.in](mailto:support@nic.in)/[antivirus@nic.in](mailto:antivirus@nic.in)

Q.22 How to protect your systems from virus infection even if no anti-virus software is yet installed on them?

Keep an eye on all the updated patches at OS level, application level

Open your emails with due care (knowing that it hasn't come from unwanted source, the incoming email is not a bogus one)

Q.23 Virus library?

### What is Malware?

Malware – short for malicious software – refers to any malicious or unexpected program or code such as viruses, Trojans, and droppers. Not all malicious programs or codes are viruses. Viruses, however, occupy a majority of all known

malware to date including worms. The other major types of malware are Trojans, droppers, and kits.

Due to the many facets of malicious code or a malicious program, referring to it as malware helps to avoid confusion. For example, a virus that also has Trojan-like capabilities can be called malware.

### **What is a Trojan?**

A Trojan is malware that performs unexpected or unauthorized, often malicious, actions. The main difference between a Trojan and a virus is the inability to replicate. Trojans cause damage, unexpected system behavior, and compromise the security of systems, but do not replicate. If it replicates, then it should be classified as a virus.

A Trojan, coined from Greek mythology's Trojan horse, typically comes in good packaging but has some hidden malicious intent within its code. When a Trojan is executed users will likely experience unwanted system problems in operation, and sometimes loss of valuable data.

### **What is a Virus?**

A computer virus is a program – a piece of executable code – that has the unique ability to replicate. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. They can attach themselves to just about any type of file and are spread as files that are copied and sent from individual to individual.

In addition to replication, some computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage. If the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer.

Several years ago most viruses spread primarily via floppy disk, but the Internet has introduced new virus distribution mechanisms. With email now used as an essential business communication tool, viruses are spreading faster than ever. Viruses attached to email messages can infect an entire enterprise in a matter of minutes, costing companies millions of dollars annually in lost productivity and clean-up expenses.

Viruses won't go away anytime soon: More than 60,000 have been identified, and 400 new ones are created every month, according to the International Computer Security Association (ICSA). With numbers like this, it's safe to say that most organizations will regularly encounter virus outbreaks. No one who uses computers is immune to viruses.

### **Life Cycle of a Virus**

The life cycle of a virus begins when it is created and ends when it is completely eradicated. The following outline describes each stage:

### Creation

Until recently, creating a virus required knowledge of a computer programming language. Today anyone with basic programming knowledge can create a virus. Typically, individuals who wish to cause widespread, random damage to computers create viruses.

### Replication

Viruses typically replicate for a long period of time before they activate, allowing plenty of time to spread.

### Activation

Viruses with damage routines will activate when certain conditions are met, for example, on a certain date or when the infected user performs a particular action. Viruses without damage routines do not activate, instead causing damage by stealing storage space.

### Discovery

This phase does not always follow activation, but typically does. When a virus is detected and isolated, it is sent to the ICSA in Washington, D.C., to be documented and distributed to antivirus software developers. Discovery normally takes place at least one year before the virus might have become a threat to the computing community.

### Assimilation

At this point, antivirus software developers modify their software so that it can detect the new virus. This can take anywhere from one day to six months, depending on the developer and the virus type.

### Eradication

If enough users install up-to-date virus protection software, any virus can be wiped out. So far no viruses have disappeared completely, but some have long ceased to be a major threat.

#### Q.24 How to disable hidden filename extensions?

For Windows 2000 users, uncheck the "Hide file extensions for known file types" and "Hide protected operating system files" and check "Show hidden files and folders" options in the view tab of Folder Options under the Tools menu in control panel. For earlier versions of Windows, uncheck the "Hide files of these types" and "Hide file extensions for known file types" and check "Show all files" options in the "View" tab of Options under the "View" menu in control panel. Additionally, you must remove all occurrences of the "NeverShowExt" value in your registry. Follow these steps to do so:

- Open the Windows Start menu
- Select "Run" and enter "regedit" to open the registry editor
- From the "Edit" menu, select "Find"
- Uncheck the "Keys" and "Data" entries under "Look at", and insure the "Values" entry is checked
- Enter "NeverShowExt" in the "Find What" box and click "Find Next"

- When a value is found, right click on the value name and select "Delete"
- Press F3 to find the next occurrence of "NeverShowExt".
- Repeat the previous two steps until all occurrences of "NeverShowExt" have been deleted from the registry
- The computer will need to be rebooted for changes to take effect

Q.25 Windows Scripting Host in Win2k Professional/Server?

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows Script Host\Settings

To enable Remote WSH, set the value of Remote to 1;

To disable Remote WSH, set the value to 0

Q.26 Anti-virus software for dial-up (not connected to NIC network at any point of time) clients?

PC-Cillin is used for remote clients (dial-up) or home users.

<http://www.trendmicro.com/en/products/desktop/pc-cillin/evaluate/overview.htm>

To download an evaluation copy: -

<http://www.trendmicro.com/en/products/desktop/pc-cillin/evaluate/trial.htm>

Q.27 Where to get the anti-virus software (OfficeScan and ServerProtect)?

From NICHQ. In the eventuality that you cannot, the trend sites are as under:

OfficeScan: -

<http://www.trendmicro.com/en/products/desktop/osce/evaluate/trial.htm>

ServerProtect: -

<http://www.trendmicro.com/en/products/file-server/sp/evaluate/trial.htm>

Q.28 How to update the TSC on OfficeScan and ServerProtect?

Check the respective documentation available at NIC support website

<http://support.nic.in> and/ or write an email to [support@nic.in](mailto:support@nic.in)/[antivirus@nic.in](mailto:antivirus@nic.in)

Q.29 How to use Sysclean.com?

This self-extracting archive is a stand-alone fix package that incorporates the Trend Micro System Cleaner. It replaces the traditional fix tool by addressing a wide variety of system infections rather than a specific malware infection.

This tool supports the following features:

- o Terminate all malware instances in memory
- o Remove malware registry entries
- o Remove malware entries from system files
- o Scan for and delete all malware copies in all local hard drives

#### How to Use

1. Create a temporary folder and copy SYSCLEAN.COM into this folder.  
NOTE: This temporary folder should be created on a local or mapped drive.
2. Download latest pattern file. Extract the downloaded ZIP pattern file into the created folder.
3. Close all applications running on your system, including any antivirus software.
4. Run the executable file, SYSCLEAN.COM, by either:
  - a. Double-clicking the tool in Windows Explorer.
  - b. Executing it via command prompt using syntax based on the aforementioned parameters.
5. Enable any antivirus software that is installed on your system and perform a manual scan.

NOTE: This fix tool generates the log file, SYSCLEAN.LOG, in its current folder.

Q.30 How to disable System Restore feature on Windows XP and ME?

The following procedure disables the System Restore feature:

#### **For Windows ME**

1. Right-click the My Computer icon on the Desktop and click Properties.
2. Click the Performance tab.
3. Click the File System button.
4. Click the Troubleshooting tab.
5. Select Disable System Restore.
6. Click Apply > Close > Close.
7. When prompted to restart, click Yes.
8. Press F8 while the system restarts.
9. Choose Safe Mode then hit the Enter key.
10. After your system has restarted, continue with the scan/clean process. Files under the \_Restore folder can now be deleted.
11. Re-enable System Restore by clearing Disable System Restore and restarting your system normally.

#### **For Windows XP**

1. Log on as Administrator.
2. Right-click the My Computer icon on the desktop and click Properties.
3. Click the System Restore tab.
4. Select Turn off System Restore.
5. Click Apply > Yes > OK.
6. Continue with the scan/clean process. Files under the \_Restore folder can now be deleted.

7. Re-enable System Restore by clearing Turn off System Restore.

Q.31 Virus scanning of Digitally signed emails?

All versions of InterScan VirusWall for Unix can scan a digitally signed email message and its attachments for viruses as long as they are not encrypted

Q.32 How do I Know that my PC is virus infected

- People reporting that they are getting emails, but, you never send them
- File size is getting increased unknowingly
- Processing power becomes too slow
- Application response time getting increased dramatically
- PC hangs now and then
- Floppy drive, CD ROM drive, etc. stops working

Q.33 How do I be assure that my PC is virus free after Installation of Antivirus S/w?

- Make sure you are having all the latest patches/ updates of OS and applications
- Make sure you are running the latest anti-virus software on your system
- Make sure the anti-virus system you are running have the latest updated pattern file and scan engine
- Take necessary pre-cautions and due care

Q.34 Where to ask for the anti-virus software license, in order to upgrade your installation from an evaluation (30-day) to a full registered version?

Write an email to [antivirus@nic.in](mailto:antivirus@nic.in)