Daly Computer Services
January 16

Type of Service:	Computer Repair
Date of Service:	January 13 – 16
Customer:	Client-3
Computer:	Gateway MFATXNIN ESX 300S CEL Intel (Essex) Celeron - 2.0 GHz (400MHz) DDR 512MB - PC266B 32X8 – Main Memory 40 GB Hard Drive HLDS 48X/24X/48X IDE CD-RW Drive 1.44 Mb Floppy Drive Gateway V.92 Half-Height PCI Soft Modem R2 (Palmer)
Serial:	xxxxxxxxxx

Services Performed:

Investigated inability to go to the internet. Found several Trojans and viruses. 1611 cookies were removed and 40 occurrences of spyware were also removed. Pornography was found on the disk from free xxx video clip.aebn.net. A secure32.htm local page was in place as the home page which said the computer was infected with spyware. This was a Trojan. I also noticed Trojan paytime and spysheriff on the disk. Attempts to remove the spyware and Trojans failed. The system directory was corrupted. Each removal of the files and the clean up of the registry resulted in the Trojan replicating itself. Even turning off the system restore and physical removal did not work. Other Trojans such as EGDACCESS_1056.dll, ramen.D@dl, Agent.FN@dl, Afftoolband and bridge.dll were found on the disk. The bridge.dll logs all user input from the terminal and sends the information to a remote site. I noticed many directories in the windows\system32 folder that should not be there. Based upon this examination, windows xp had to be re-installed.

Text files were saved to off-line for a later copy. The windows XP was reloaded after re-partitioning and re-formatting the disk. 5 logins were set up: User5 (admin), User4 (admin), User3 (limited), User2 (limited) and User1 (limited). Previous files were loaded back to the disk. Installed software included: Norton Internet Security, 2wire, Microsoft Office, Microsoft Works, Spy Sweeper and several windows xp power tools. The registry was modified for the limited logins so that no software can be downloaded or installed. Each user id environment was checked and set up for varying screen backgrounds and options. A shared tool bar was added to all logins. Each login was secured with the users mail password. Live update was run to install all the latest Norton fixes. Microsoft update was run to have all the up to date fixes. Microsoft office update was run to have all the update fixes for office. Security settings of downloading software was checked and verified. User instructions for monitoring computer usage were prepared.

Cost of Services Rendered:

Material Cost:	
Spy Sweeper	$ xx.xx
Office 2000 CD	$ xx.xx

Total Material Cost:	$ xx.xx

Monitoring Computer Usage

All users have folders under c:\Documents and Settings

On your computer, the following users are installed:

User1	aaaaa@zzz.net	pokrah
User2	bbbbb@ zzz.net	peanut
User3	ccccc@ zzz.net	anne48
User4	ddddd@ zzz.net	yugioh
Owner User5)	eeeee@ zzz.net	pascal1201

Periodically, clean out the following directories:

C:\Documents and Settings**<user>**\Cookies

You generally can not remove the index.dat file or desktop.ini file. Hit the ctrl-A keys to select all the files in the directory. Next holding down on the ctrl key, use the mouse to de-select the any file. This should un-highlight the file. Next hit your delete key and hit enter to remove the files.

C:\Documents and Settings**<user>**\Local Settings\Temporary Internet Files\Content.IE5

All directories under Content.IE5 and files can be removed. The directories will show you what files the internet browser copied to the disk. Before removing them you may want to quickly view the images to see what the children were doing. The http://www.myspace.com will leave lots of directories and files on your disk. Using the Internet Explorer option to clean out files will only remove files older than 1 week, so you can catch what was going on right away.

C:\Documents and Settings**<user>**\Local Settings \History\History.IE5

All MSHist* folders can be removed. They are the users history files. Don't worry about removing the index.dat file as it will be re-created. (Sometimes history is displayed as Today, yesterday, Monday etc. You can remove those directories too.

To see which exact url was visited, double click on Norton Internet Security.
Select the Statistics selections from the left side. Select View Logs from the Right side.
Now with the Log viewer displaying, click on the Firewall selection to see the date, time and user and the url selected – pretty cool! I periodically clear out the logs by doing a Log→Clear category. Norton will log everything here.
Be sure not to let the kids see you look here.

Periodically, run:

Start→All Programs→Accessories→System Tools→Disk Cleanup
Start→All Programs→Accessories→System Tools→Disk Defragmenter

Computer Name: xxxxxxxx-Gate - **User SID's**

User5	=	S-1-5-21-1343024091-1935655697-1177238915-1003
User1	=	S-1-5-21-1343024091-1935655697-1177238915-1004
User2	=	**S-1-5-21-1343024091-1935655697-1177238915-1005**
User3	=	**S-1-5-21-1343024091-1935655697-1177238915-1006**
User4	=	**S-1-5-21-1343024091-1935655697-1177238915-1007**

Restricting Users from Installing Software: (CAUTION: when using regedit)

Log on as User

Start→Run regedit

Navigate by clicking on the left pane's plus sign to drop down the tree to:

HKEY_CURRENT_USER**<SID>**\Software\Microsoft\Windows\
CurrentVersion\Internet Settings\ZoneMap\Domains

Right Click on the RIGHT PANE (empty area) New → Dword (Put * as the value)
Right Click on the value * → Modify (Put 4 as the value)

To un-do this restriction, simply delete each Dword from all 3 users (Right click on the * then delete)

Preventing Users from Downloading Files

Log on as User

Start→Run regedit

Navigate by clicking on the left pane's plus sign down the tree to:

HKEY_CURRENT_USER\<SID>\Software\Microsoft\Windows\
CurrentVersion\Internet Settings\Zones\3

Right Click on the RIGHT PANE on the value 1803 → Modify (Put 3 as the value)

To un-do this restriction, simply Modify the 1803 value (Put 0 as the value)

Installed Software:

Windows Xp Home
2wire
Norton Internet Security
Windows XP Power Tools
Microsoft Works
Microsoft Office (word, excel, power point)
Spy Sweeper

I set up windows update to download automatically. You will have to be logged in to let it install due to the installation restrictions. I ran windows update and live update to obtain all the most current updates.

Both User1 and User5 are administrators. Due to the 2wire configuration, non-administrators will receive 2 error messages when they log in (just ignore them).

The machine is set up to use both the sbc browser and internet explorer.

I copied the text files from the old disk after virus checking them and put them under the kids or your directory.

Should you have a problem in accessing the internet – don't turn off Norton. Worst case scenario is to pull the internet cable from the computer, remove Norton, then reinstall Norton. After Norton is installed, run live update again. I have seen some computers used as a porn server where the owners were not aware of it. These computers are usually trashed and no files can be saved.

I created a directory called: c:\My Applications. I try to install everything in this directory. This way, applications won't conflict with the Microsoft OS. Norton is installed under:
C:\My Applications\Symantec\Norton Internet Security.

Should you have any questions, feel free to call:

Garry Daly