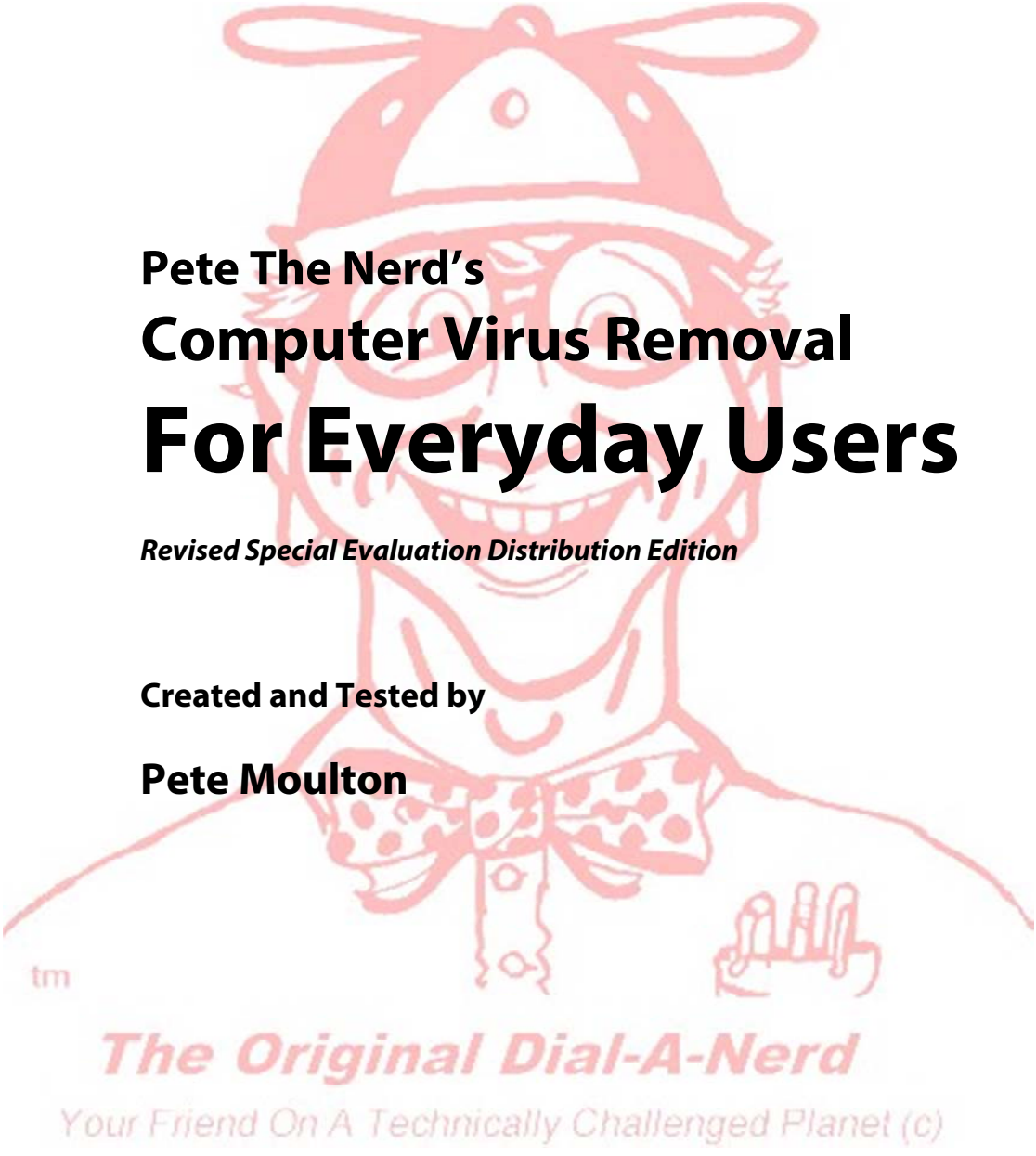


Pete The Nerd's

Computer Virus Removal

For Everyday Users

Revised Special Evaluation Distribution Edition

Created and Tested by

Pete Moulton

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Copyright © 2011-2012 by Pete Moulton

All rights reserved Worldwide. No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means including electronic, magnetic, optical, manual, or otherwise without prior written permission of P. D. Moulton, 7146 Rivers Edge Road, Columbia, Maryland 21044 -- Phone 800 432-6373. If you wish to use parts of this material, please email me for permission. Thank you.

ISBN:
ISBN-13:

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Dedication

This book is dedicated to all computer users that are the hapless victims of virus and malicious software attacks. It is also dedicated to my dad, Doug Moulton, the hardest working man I ever knew. His work ethic was passed on to my brother George, his wife Martha, and their son Josh. I could not forget Cate Dolan, the love of my life, and her autistic grandson Paddy Dolan. Such people are the salt of the earth.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Contents

Preface *7*

EXECUTIVE SUMMARY *11*
- Book Focus 12
- The Task 12
- Challenges 13
- Learning Approach 14
- Understanding Computers 15
- Topics Covered 17
- Summary 18

CHAPTER 1 Virus Background *21*
- How Viruses Started 22
  - The Origin of Viruses 23
    - Viruses Are Programs 23
    - Why Create Viruses 23
    - One Step Ahead 24
    - Cost Not Related to Effectiveness 24
  - How Viruses Infect Your Computer 24
    - Infection From Web Sites 25
    - Web Link Testing 25
    - Typical Virus Attack 26
- Universal Internet Virus Removal 28
  - One-Click Limitations 29
  - Some Things A Computer Just Can't Do Well 30
  - A Middle Ground 32

CHAPTER 2 Virus Removal Software Tools *33*
- Purchased Virus Protection 34
- Software Tools 35
  - Spybot - Search & Destroy 40
  - Malwarebytes® 41
  - AVG® Antivirus 42
  - Super Antispyware® 45
  - EASUS® Partition Manager Free 45
  - Other Tools 45

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Summary 46

CHAPTER 3 Virus Removal Step By Step 47
Virus Names 48
Virus Removal Steps 49
Installing Virus Removal Tools 49
Basic Procedure 50
Step 1 – Boot into Safe Mode 51
Step 2 – Download, Install and Run Malwarebytes® 58
Step 3 – Download, Install and Run Spybot Search & Destroy® 59
Step 4 – Download and Run Super Antispyware 66
Step 5 - Rebuild The Master Boot Record 68
Step 6 –Complete Safe Mode Virus Removal and Review Results 70
Step 7 – Remove Temporary Files from the Computer 71
Removing User Account Temp Files with the Command Console 71
Removing User Account Temp Files with the Windows® Explorer 76
Step 8 – Reboot and Repeat Step 2, Step 3, and Step 7 in Normal Mode 91
Step 9 – Repeat for Each User Account 92
Step 10 – Check and Restart Your Virus Scanning Software 93
Summary 96

CHAPTER 4 Virus Mop Up 101
Virus Removal Residual Problems 102
Virus Aftermath Cleanup 103
Damage Type 1 – Internet Explorer Cannot View Any Web Sites 104
Damage Type 2 – EXE Files Do Not Run 111
Damage Type 3 – Your Data Has Disappeared 121
Damage Type 4 – Your User Account Is Damaged 139
Summary 142

CHAPTER 5 Rebuilding Windows® 145
Reinstallation Thoughts 146
Rebuilding Windows® 147
Reinstallation Caveats 148
Windows XP® Reinstallation 149
Reinstalling Windows® Over Windows® 150
Complete Windows XP® Reinstallation 153
Windows 7® (or Vista®) Reinstallation 154

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Windows 7® Startup (Boot) Repair....154
Windows 7® Complete Reinstallation....156
Summary....160

CHAPTER 6 Virus Prevention....161
Nerd Tales....162
Virus Prevention....163
Web Surfing Rules....164
No Free Lunch....164
Avoid Speed Up Programs....165
Remove All "Evil" Tool Bars....167
Clean Up Your Computer Weekly....167
Uninstall Unneeded and Seldom Used Software....169
Summary....172

Conclusion....173

About The Author....177

Disclaimer....179

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Preface

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

In 1 hour of your time and for the cost of this book you can remove viruses, malware, and spyware from your computer speeding it up. This can save you $50 or more. Chapters 2 and 3 present a step by step cookbook virus removal procedure. They identify the best free malware, spyware and virus removal software tools.

An everyday user who knows little about computers and is attempting to remove viruses their computer for the first time, may find that this book is not an easy read. However, there are non-technical explanations and analogies of how a computer works and how to remove viruses that even the most naive user can understand. Other explanations do have necessary technical details in them. Do not sweat the details, just get the overall picture. Give that some time to sink into your understanding of computers. Next implement the steps one step at a time slowly to perform the virus removal process. You can do it if you are patient and a little persistent. In this manner, the most inexperienced and non-technical person can get the most out of this book.

Everyday users following the steps in this book can save their data and remove viruses from their Personal Computers restoring them to normal operation. The book explains in plain non-technical language using easy to understand analogies how to thoroughly remove viruses, malware and spyware.

A quick read of this book helps the most naive and timid non-technical readers avoid added damage during a virus attack. The virus removal procedure presented can be followed by everyday users so they successfully remove most all minor and moderate viruses. Technical readers are able to remove more complex and nastier viruses.

When an everyday user hires someone to perform virus removal, this book helps those users understand how a professional completely and thoroughly removes viruses from their computer.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

The virus removal tools used in the procedures described in this book can be downloaded from the Internet. They are free for personal use.

Thank you for consider reading this book. My goal is to help all computer users. Reading this book helps me add to the For Everyday User series. The next planned books are: 1. Pete The Nerd's How To Speed Up Your Slow Computer For Everyday Users, and 2. Pete The Nerd's Network Repair For Everyday Users.

Please tell your friends if this book helps you or email me at: **dialanerd@verizon.net** if you have questions. Thank you.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Please use for notes.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

EXECUTIVE SUMMARY

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Book Focus

This book has a single simple focus, showing everyday users how to effectively remove viruses, malware, and spyware from their Personal Computer (PC) for an investment of 30 minutes. The book presents a step by step cookbook approach in chapters 2 and 3 that everyday users can follow. Chapter 2 first identifies effective virus removal software tools and then Chapter 3 walks you through a step by step cookbook procedure to remove annoying computer viruses, malware and spyware. These free for personal use software tools when used in combination with the procedure presented here can return most computers to normal operation.

The approach is to show everyday users how to remove viruses from their computer by using free virus removal software tools on the infected computer. The computer should have a working high speed Internet connection.

The Task

This sounds simple, but it is not. After starting the book, three computers were presented to me infected with viruses. With great bravado I began to remove the virus infestation from the first computer only to discover that no programs (EXE files) would run on the computer even in Windows® Safe Mode. It was a humbling experience. This caused me to think harder. When it comes to computer viruses I always remember what my first ex-wife said to me whenever we had an argument: "I will win!" She always did! So with viruses I keep repeating that mantra "I will win, I will win". Yes, I did win! So can you with this book!

The tools that professionals often use to remove viruses from computers are specially configured computers. The disk drive of a virus infected computer is quickly installed in these computers as an additional disk drive. This permits attacking the infected drive and removing the virus

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

files using a version of Windows® that is virus free. The virus infected computers themselves are used to remove the viruses to complete the process after the initial virus files have been identified and removed by the specially configured computers.

Challenges

Challenge number one is removing viruses using the virus infected computer by itself. Next the software tools that remove the viruses in this educational book have to be "free for personal use" programs found on the Internet. **Challenge number two** is showing you where to find, install them, and then how to run them so that they remove viruses.

Viruses are very tricky and can often corrupt Windows® beyond simple virus removal repair. So removing viruses from a computer without professional tools appears at first blush to be a piece of cake. With only the virus infected computer and a functioning high speed Internet connection, this becomes a significantly more difficult exercise than one expects. Removing live viruses without special tools helped develop and hone my logical thinking and strategy used to remove those viruses. All real virus removal problems can be solved, but it is always a knowledge expanding experience to battle to the death new computer viruses. Consequently, this book is not just aimed at a step by step procedure that removes viruses from your computer, but rather aimed at giving you the logical thinking skills and knowledge to attack any virus you encounter.

The procedure presented uses drawings of screen captures to assist in performing virus removal on your computer. Because I am a picture person, when you give me a list of steps to follow I become lost. But give me a map or some pictures to follow and I know where I am and I am good to go. So the steps presented here have drawings of screen captures to help guide you.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Learning Approach

When I taught computer repair, we would describe the Air Force and the Navy approach to fixing electronic systems. The Air Force would present a problem with symptoms a, b, and c, then say that replacing Unit X would fix the problem. In contrast the Navy would show how the system worked – what component preformed what function, then say OK now go fix the system. This makes a good story, but I am not sure it is truly representative of Air Force and Navy training.

When removing viruses there is no precise procedure because each problem is different. This means that we like it or not must follow the Navy approach to solving the problem. In this book we give you tools to find and steps to follow along with good strategies or methods of attack that can successfully remove viruses from your computer. However, you will have to adapt them to the problem at hand because every virus removal is different. There are no set rules. You will need to step back from time to time and ask yourself: "Have I gone too far down this rat hole?", "Should I just stop here and try a totally different approach?", and "Should I use the nuclear option and just rebuild Windows®?"

Nerd Tip: *If you think that your computer has been hit by a virus, stop right there and remove it. The longer viruses run unchecked in a computer, the more damage they inflict on Windows®. This damage ultimately requires that Windows® is reinstalled on the computer. While Windows® installation is a straight forward task, it is easily complicated by saving all your important data, reinstalling all your purchased software, and reconfiguring Windows® with your personal preferences. Also any virus removal program asking for money to remove viruses from your computer is most likely a virus itself. So never pay such blackmail.*

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Understanding Computers

When you understand computers, you can understand how viruses attack your computer. Computers are not hard to understand. For example, imagine yourself at work. At the beginning of the day you sit at your desk. There is a filing cabinet next to the desk. The top of the desk is empty and the files you are going to work on during the day are locked and stored in the filing cabinet next to the desk.

The top of the desk is equivalent to the Random Access Memory of your computer. It is the working area of the computer just like the top of the desk is the working area you use every day.

The filing cabinet is the permanent file or information storage repository for your work. This is similar to the hard disk drive in your computer being the permanent filing cabinet for all the data on your computer.

Every day at the end of the day the top of the desk is cleaned off and all the files are stored in the filing cabinet overnight. When you begin work the next day, the files are removed from the filing cabinet and placed in the working area on the top of the desk.

This desktop and a filing cabinet analogy demonstrates how Windows computers work. The top of the desk is the Random Access Memory (RAM) or the working area of the computer. The disk drive is the filing cabinet or permanent memory in the computer where everything is put when the computer is powered off.

When we turn on a computer, we start with an empty desktop and a full filing cabinet. The first thing that a computer does is it goes to the Read Only Memory (ROM) – a note permanently burned into the wood on the desktop. It tells the computer to go to the filing cabinet and open the top drawer, first folder and the first paper list in the folder (this is called the Master Boot Record – MBR). The MBR is always located at address 0, the universal starting address for all computers.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Windows programs are lists of instructions written on paper in the file cabinet. The first list tells the computer about the disk drive and the second list right next to the first list tells the computer to get more lists from the file cabinet. These lists are in different drawers and in different files. The computer puts these lists and other papers containing data on the desktop.

Small desktops (computers with less than 512 MB RAM) fill quickly, and larger desktops (3 GB RAM and up) fill more slowly. Lists on the desktop are at our fingertips and can be accessed quickly while other lists remaining in the file cabinet take longer to find and must be placed on the desktop for the computer to work with them.

When the desktop is filled, the computer puts lists in an easy to reach location in the file cabinet – the top drawer second folder. As work goes on more and more lists are put in that location. As the computer works for us, it finds that information it wants is not on the desktop so it goes first to the top file cabinet drawer second folder and checks to see if it is there. When it is it is brought to the desktop, but now the desktop is full so something on the desktop must be placed in the top drawer second folder to make room for the list placed on the desktop. This happens a lot with Windows especially when the desktop (RAM) is small. The constant swapping between desktop and file cabinet slows down the computer.

Sometimes a nasty virus sneaks into the office and places a bad list in the file cabinet. The computer takes that list and does what is on it. The bad list says eat lunch, make a phone call, and then jump out the window. Since the computer does not know any better it jumps out the window as instructed and we see bad things happen.

Hopefully, you are beginning to understand some more about why your computer behaves as it does. My point is that it is never hard to understand computers when someone makes it simple. Also this

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

explanation should help you put into perspective the steps in the virus removal procedure presented in Chapter 3.

Topics Covered

This book covers:

Chapter 1 – Virus Background

Chapter 2 – Free Removal Tools

Chapter 3 – Virus Removal Procedure

Chapter 4 – Virus Aftermath Cleanup

Chapter 5 – Rebuilding Windows®

Chapter 6 – Virus Prevention

Each chapter provides specific information learned over the last 30 years working on computers.

In my experience, if you know most everything about a subject, you still can learn something from someone else. So I believe that even the most knowledgeable people reading this book can learn something.

My commitment to you is that this book contains almost everything that I have learned technically on how to remove viruses and other malware from your computer. The book explains in clear, direct and simple terms how to remove malware (spyware and viruses), restore Windows®, and save important data.

Included are Internet links to the free for personal use software tools that effectively remove viruses and malware from your computer. This minimizes your research and repair time. Repair procedures compliant with software licensing and virus removal software that really works are identified exactly. Internet links permit you to easily find them, download

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

them and remove viruses from your computer. Some of these tools change over time. What is a good tool today may be much less effective in three months. As these changes occur, please e-mail me at dialanerd@verizon.net so that I may make sure you the best tools.

This book is intended to be short and focused on the single problem of virus removal from your computer while saving your data. You should be able to complete the virus removal without assistance.

Summary

If you need to remove a virus, Chapter 2 identifies highly effective software tools and points you to where you can download them. Chapter 3 provides the step by step procedure to follow employing these tools to start and complete the first part of the virus removal process. Chapter 4 goes beyond the special tools and covers what to do when viruses corrupt Windows®. Chapter 5 gives you the step by step approach to repairing all versions of Windows® that has been damaged by viruses and malware. Chapter 6 concludes this book by giving you the periodic maintenance procedures that when followed help prevent future virus attacks.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

To begin your computer must at least be running and have Internet access. Alternatively, use another computer to gather the required tools and a thumb drive to carry them to the virus infected computer.

So let's get started and have some fun along the way.

Enjoy.

Pete

Dial A Nerd

Your Friend on a Technically Challenged Planet©

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Please Use This for Notes.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

CHAPTER 1
Virus Background

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

How Viruses Started

The first virus I removed from someone's computer was the Kelz virus. This virus ruled in the days of Windows 95® and Windows 98® which were computer Operating Systems built on a foundation of DOS (the original PC Disk Operating System). My lawyer at the time got his main computer infected with Kelz.

Please understand that my lawyer was the king of the world. In his eyes I was a lowly serf. Well at least a serf that solved computer problems. My lawyer always tried to solve his computer problems without calling me. So I got to fix problems like speakers not working because they were plugged into the microphone jack on the sound board and not the speaker jack. I enjoyed his reaction when I explained to him how I solved the problem.

The Kelz virus on my lawyer's computer was almost impossible to remove. After spending a day trying to identify the virus and remove it using virus scanning software on his computer, it finally dawned on me that the (several bad words apply here) Kelz virus had lodged itself in a location on the disk drive where it always got into memory first and prevented its detection and removal from the computer. I was making no progress until the thought occurred to me that I could scan his disk drive across my Local Area Network using another computer. As long as I did not give his computer access to that computer's disk drives but only shared the disk drives on his computer this was a relatively safe procedure. When the drive was scanned in that manner, the Kelz virus was identified and the root Kelz virus was removed. Then the specific virus removal tool for the Kelz virus could be downloaded, run and used to clean up his computer completely. This turned out to be a two day job.

As a result, I developed special virus removal computers that scan disks from virus infected computers, detect viruses and remove them. This provides a starting point virus removal. Complete virus removal also

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

requires running programs on the virus infected computer. The special virus removal computers also make an image (an instant photograph) of the infected computer's disk drive so that if anything goes awry in the virus removal process and data is lost, there is copy that can recover it and restore the drive to its original virus infected state.

In this book you learn how to remove viruses from your computer without using special virus removal computers.

The Origin of Viruses

Modern computer Viruses were first created as a college assignment back in the early 1980's. This is described on Wikipedia.org at this link http://en.wikipedia.org/wiki/Fred_Cohen.

Viruses Are Programs

A virus is simply a computer program that copies itself and spreads these copies to other computers. This is essential for the survival of the virus. Similar to any other viral or bacterial disease, all viruses replicate and infect. Today's viruses do more. They hide and mask themselves as Windows® software components, they damage Windows® making the hapless computer user go crazy with frustration, and they try to extract money from computer owners and Internet advertisers.

Why Create Viruses

Some viruses can make money by driving traffic to specific web sites. These sites make money based upon the number of visitors coming to the site. They get paid by advertisers for the number of times you click your mouse and view pages. The virus or spyware makes your Web browser (Internet Explorer or Firefox) point at those sites so you are likely to view their web pages. In this case they are infecting your computer so that evil Internet sites make money off of Internet advertisers.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

One Step Ahead

The difficult part of virus removal is that the viruses are always one step ahead for the tools that remove them. Since they are created continually by some geek (geeks are circus freaks and nerds come from Dr. Seuss) in order to achieve 15 minutes of fame, the tools to remove them are a step behind the virus creation. Virus removal tools can only be updated after the virus is detected and identified by its victims. Virus removal tools must play catch-up to identify and then remove the viruses impacting your computer. This means that they are updated frequently perhaps daily. Most tools are highly effective and do a very good job.

Cost Not Related to Effectiveness

The cost of virus removal software does not relate to its effectiveness. Expensive removal tools are no better than free or less costly ones.

One tool alone is not sufficient to remove all viruses. Several tools can be run on the same computer and all will find and remove viruses and spyware.

Viruses fall under the classification of malicious software or malware. Spyware and other advertising software are also considered malware. Virus removal tools also remove malware.

How Viruses Infect Your Computer

Originally computer viruses were spread by infected floppy disks. Virus removal programs were posted on bulletin board computers and downloaded using dial-up communications over the telephone network. My first virus infection was transmitted by a 5.25-inch floppy disk.

An infected floppy was most commonly a bootable floppy disk that loaded the computers disk operating system (DOS). Alternatively, a virus could add itself in a legitimate program and then loaded when the legitimate

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

program's executable (EXE or COM) file was opened. Once the virus was in memory, it wrote copies of itself on every floppy that was placed into the computer's floppy disk drives.

Popular software or "free" software transferred into a computer electronically via a bulletin board or an Internet download soon surpassed the floppy disk virus transfers. In the 90's other viruses written in scripts used in Microsoft® Office programs such as Word or Excel. Office (DOC and XLS) files carried these viruses from computer to computer. Microsoft® Outlook email messages infested with viruses spread viruses from computer to computer. Current e-mails block the transfer of executable (EXE and COM) files. Other script files are scanned as they travel through the Internet. E-mail messages today are virus free with a caveat.

Infection From Web Sites

All web sites run programs in your computer. These programs produce striking visual effects on web pages. They can also infect your computer with a virus. So e-mail messages carrying links to web sites may not be infected with a virus but the links may direct you to web sites where your computer can be attacked and infected by viruses. Any instant message or e-mail pointing you to an unknown site puts your computer at risk of virus attack.

Web Link Testing

Virus scanning programs today are testing web links to provide protection against virus infection. Some virus programs provide Internet Domain Name Service (DNS) servers that prevent you from visiting known virus risky web sites.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

For example, I have a little white Saturn that is third cousin to a Yugo. This Saturn model is notorious for not starting in cold weather because of the dielectric grease in the starter switch.

To solve this problem I was replacing the starter switch. In the process of trying to determine the exact part and how to replace it, the Internet was searched. While looking for videos and pictures linked to the youTube.com site, my poor computer hit a virus. This was a money extracting virus displaying the alarming message "Your computer Infected by a Virus!!!" The message is the virus. My mistake was to click on the upper right corner red X for exit instead of just pulling out the power plug. By trying to exit, the virus gained a greater foothold in my computer. Needless to say the bad four-letter words started flying because I knew my mistake and the time now required to remove the virus. This is typical of viruses that come from web site links. The web site, youTube.com, is a safe site, but links from it to other sites are not necessarily safe.

Nerd Tip: *Microsoft® was once good for the computer industry because their Windows® monopoly standardized computer software, lowered prices and exploded the purchase of computers and networking components. However, because of this technology monopoly Microsoft's Internet Explorer has become the most virus attacked web browser. Microsoft's web browser uses a scripting language called ActiveX. A Silverlight and other scripting languages are replacing ActiveX in newer versions of Internet Explorer.*

A safer web browser is Firefox. Firefox is a General Public License (GPL) free web browser. It uses Java as a scripting language. It is less attacked than IE, so while not absolutely free of virus attack, it is less attacked.

Typical Virus Attack

A typical virus attack on a customer computer is shown in Figure 1 - 1 Virus Attack. The virus splattered misleading messages all over the

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

display. Any time the CONTINUE or CANCEL button was hit, a new error message appeared. The warning of damage to the computer hardware was completely false. One virus message had the word Failed spelled as Filed (Windows – Delayed Write Filed). The big hidden message was a scanning message to make you believe that it was useful software when in fact is was doing nothing. These viruses disguise themselves as coming from Microsoft® when in fact they do not.

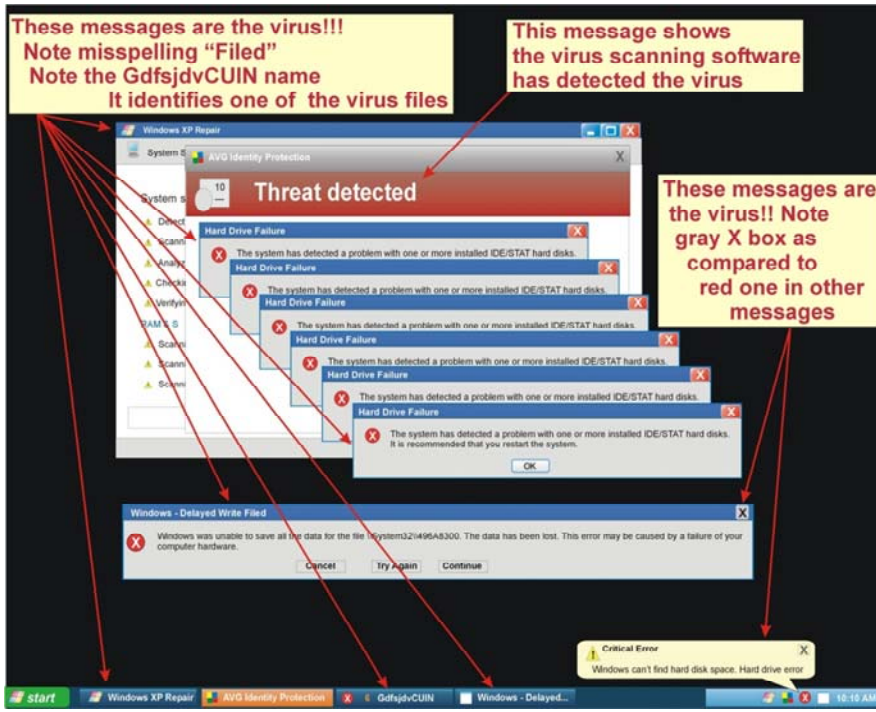


Figure 1 - 1 Virus Attack

In this case the AVG antivirus software detected the virus and popped up an error message. While it tried to remove the virus, additional software scans by other programs were needed to return the computer back to proper operation.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

This virus made data disappear by marking files as System – Read-only – Hidden. In this manner, it was attempting to convince the user that the drive was damaged and the data was lost. This was in fact false.

At this point the best thing to do is to pull the plug and perform the virus removal procedure presented in Chapter 3. Trying to continue further with this computer only causes the virus to do more damage to the computer and Windows®.

Universal Internet Virus Removal

Universal Internet Virus Removal programs are advertised continuously on TV. One of the early programs was finallyfast.com. When testing this program I discovered that it found problems with my computer no matter how clean it was. When I ran several programs to improve the computers performance and to clean up various areas of the computer, the finallyfast.com program found fewer problems but continued to report many problems with the computer. The programs I ran removed large amounts of unnecessary data from the subject computer. This data was not picked up by finallyfast.com. In order to complete the finallyfast.com cleanup process, it was necessary to pay an additional $139.

The newest program to be advertised in this manner comes from PCpitstop.com. It is called PCmatic. The PCpitstop.com site differentiates itself from other virus removal programs because it uses what is called "Cloud Computing" to retain virus identification signatures on the Internet. It uses special servers organize all the information it finds on viruses from every computer that uses PCmatic. Further, it uses both a "blacklist" combined with a list of good software to detect and block viruses.

The good news with the PCpitstop.com site is that on their virus removal cost was a one-year subscription advertised at $49.99 for 10 installations. This is less expensive than the annual subscription for the cheapest

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

antivirus software, several other well-known antivirus programs, and certainly much less than $139. Free for personal use antivirus programs like AVG antivirus are equally effective and one cannot beat the price.

Because of copyright restrictions, the PCpitstop.com site's webpage cannot be shown as figure in this book. When examining the page, and looking through most of the links, I discovered the top 25 spyware and adware programs listed. This list is symptomatic of the problem that virus removal software presents. It was last updated according to the website on February 25, 2008. Although many of the viruses listed are still problems today, a two-year-old list is obsolete.

One-Click Limitations

In my mind it remains to be seen whether the PCpitstop.com site's "Cloud Computing" and good software list approach truly does a more effective virus detection and removal job. Here's why.

Spyware has defined files that disguise themselves by using file names which seem like legitimate Windows® program filenames. These filenames do not change often. Consequently a spyware removal program can look for those names in the Registry and INI files stored on the computer. When it finds one of those filenames, it can then more thoroughly test the file to verify that it is indeed spyware.

Viruses are rogues. They don't care about using filenames similar to Windows® filenames to hide themselves on a computer. Viruses create filenames from random numbers and letters so that they are different each time they are created. (Please see the beginning of Chapter 3 for more information on virus names.) Viruses also encrypt themselves to hide on the computer. This makes scanning for viruses more difficult. To detect such viruses each file must be scanned and searched for the small part of the virus that is not encrypted and uniquely identifies that virus. As stated earlier viruses are one step ahead of virus detection software

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

because virus protection software must first analyze reports to determine how to identify it on any computer. No matter how effective the identification process is there is always a lag of at least a week between the time when a virus is first discovered and the virus removal software catches up and can remove it. That's why virus removal software is often updated daily.

Good software also changes continually. New products and product updates are released on a periodic basis. Use Microsoft® for example. There is all most always a new Windows® update released each day or certainly each week. If you're good software update is not on the good software list maintained by the PCpitstop.com site, your important program could refuse to run. While the PCpitstop.com site permits you to run the program, it is confusing when important programs fail to respond as expected.

Some Things A Computer Just Can't Do Well

Finally, there are things a computer program just can't do as well as a human being does. Examining your disk drive for viruses by spotting strange files based upon their file name, testing them to see who created them, and then deleting the files, are in many cases more effectively done by a thinking human being than by a program designed to test for viruses. This is better understood after reading Chapters 3 and 4. Further, over the Internet virus removal software cannot check for hardware errors like popped capacitors. See Figure 1 – 2 Popped Capacitors. In the picture just below the CPU fan and below the red inductor coils are two brown and sliver topped popped capacitors. The tops are bursting open like microwave popcorn bursts when it is cooked. Below the left popped capacitor at the bottom of the picture to the left of the purple-pink connector is a black and silver capacitor that is not popped. Its top is sunken-in like there is a vacuum pulling it down.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

When the capacitors on the computer's main logic board pop or fail, the computer behaves erratically. It may work one minute and then fail the next. This mimics virus behavior. No over the Internet virus software is able to my knowledge detect popped capacitors. Detecting popped capacitors is simple, just remove the side of the computer case and use a flash light to visually inspect the top of every capacitor you can see. As a nerd I visually inspect every desktop computer and run CHKDSK /F on every disk drive before proceeding to perform a virus removal. In this way no customer spends money on virus removal when the source of a problem is computer hardware failure.

For simple virus removal, a straightforward procedure using several virus removal tools as described in this book should effectively complete the job. These virus removal tools can be downloaded for free off the Internet. In cases where Windows® is corrupted beyond simple repair, then rebuilding Windows® is the quickest and best solution. This is often done by system recovery files installed on the computer's disk drive, or by reinstallation CDs. The only trick is how to save your data and recover your important programs.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

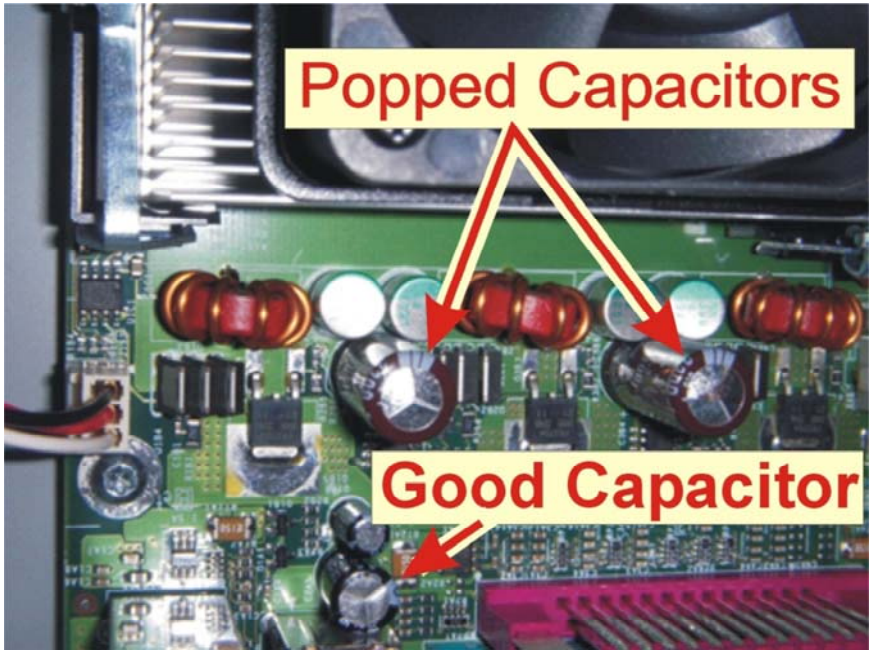


Figure 1 - 2 Popped Capacitors

A Middle Ground

Between the extreme of simple virus removal and the extreme of rebuilding Windows® lies a middle ground where online virus tools as well as normal virus removal software work to remove the viruses and restore the computer to normal operation. This is particularly true when there is a human being that understands the concepts of virus removal watching those online virus tools and removal software complete their job. In the school of life there is no cheating. Whatever way you can solve the virus removal problem at the least cost to yourself works in real life. No single solution is a universal virus removal answer for everyone.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

CHAPTER 2
Virus Removal Software Tools

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Purchased Virus Protection

Most people already have purchased virus protection. Many times they have a year of purchased protection remaining. It is hard to explain to them, that the virus protection they purchased was compromised, and their computer is infected with viruses. In most cases, a single virus invader has invited its virus friends in for a house party like in the movie "Weird Science". Consequently, the virus protection software was corrupted by the virus and needs to be removed.

People just hate to give up the coverage they purchased in spite of its obvious ineffectiveness and corruption. They all want their money's worth. No one virus protection software is truly superior to any other virus protection software. The main issue is restoring the purchased software because a product installation key or some equivalent unlocking mechanism is needed to reinstall the software. Also, many security suites had grown in size so much that they severely impact the performance of older computers.

In many cases, it is better to start fresh than to attempt to resurrect the old security software. When you are using something that has not worked, why keep repeating the same mistake. This is like beating your head against a wall repeatedly. It is less painful when you stop, regardless what you paid for the privilege of beating your head against that wall.

Nerd Tip: *"Weird Science" loved by nerds, and hated by intellectual elites starred Anthony Michael Hall. We met briefly at Los Angeles Airport (LAX) as we passed each other taking flights to different destinations.*

Here is a good nerd quiz for you, why is Chicago O'Hare Airport's designation ORD? It was built over an ORcharD. This is a light aside to assure you that not all this book is technical terminology and procedures.

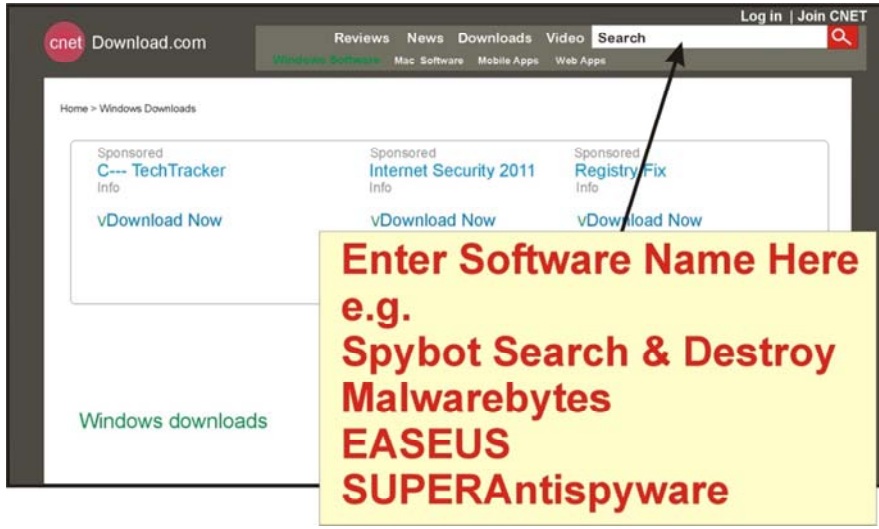
Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Software Tools

To get the software tools needed, a working computer with an Internet connection is required. Unfortunately, I cannot just give these virus removal programs to you because it violates their software licensing. That is why this book is "Do It Yourself - DIY".

There are just four or five virus removal software programs needed to clean viruses off of a computer. These tools can be found on the Internet at the http://www.download.com web site. When you use this web site name, it sends you to http://download.cnet.com/windows/. The download.com site is presented here because it is easy to type into the computer. See Figure 2 - 1. The download.cnet.com Site Home Page.

This is a good site to use for finding a variety of free software and shareware. Shareware is software that is free to try, but costs money to use. The software tools we use are free software for personal use. If these tools work for you, we strongly recommend sending the authors a contribution for their work or perhaps buying an upgraded version.



Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Figure 2 - 1 The download.cnet.com Site Home Page

CNET® software is virus and spyware free but not advertising free. The site rates the software based upon author reviews and computer user reviews. The site can be searched for free software or shareware. Sometimes you may select programs that test your computer for problems, identify problems (some identification is dubious), but then will not correct the problems or only correct a part of the problem unless you pay for the full version. In the cases where I have purchased such try before you buy programs, the paid for version did not perform satisfactorily. Consequently, freeware programs are preferred programs. When you find a useful program, please send the authors some money to help maintain that program.

Nerd Tip: *A quick way to reach a COM website is to enter its name into the address entry panel of the web browser, then hold down the CTRL key and strike the Enter key. The web browser will then automatically enter the remaining information including http://www and the COM information. Try this with Google®.*

We are going to use the search function to locate and download the software tools used. The search panel as shown in Figure 2 – 1 is in the upper right. In the panel is the word search and at the end of the panel is the magnifying glass icon in a red square.

Free effective virus and malware removal tools are:

1. Spybot Search and Destroy® (Spybot - Search & Destroy)
2. Malwarebytes®
3. AVG® Antivirus
4. Super Antispyware®
5. EASEUS® partition manager free

Type the name of these programs in the search panel. When CNET® displays the green "Download Now" button for the program, click on it.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

CNET® has a new download procedure and software that unless you are careful, results in nasty Adware being installed on your computer. The next few diagrams should show you how to avoid downloading the nasty Adware.

The first CNET® download link Window should pop up after you click on the green "Download Now" button for the program. This is shown in Figure 2 – 2 CNET® Download Step 1. You must click on the green "Next Step" button to continue.

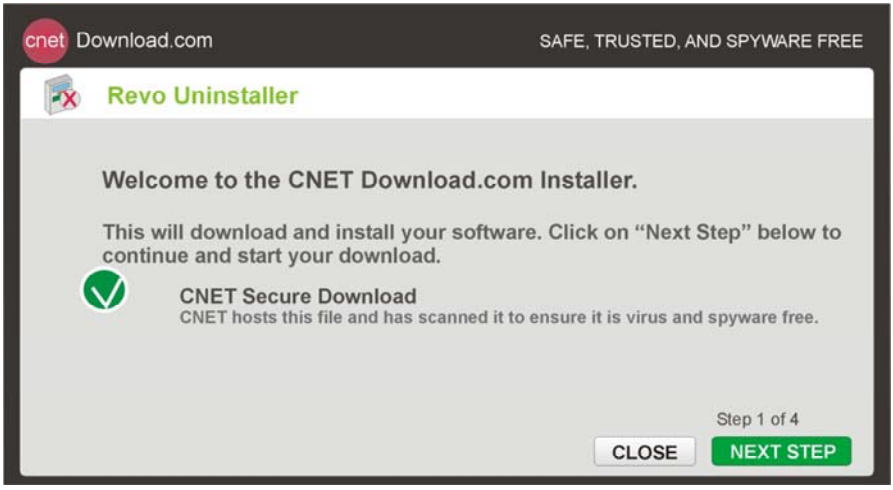


Figure 2 - 2 CNET® Download Step 1

The next Window the CNET® downloader program pops up is the Window that installs the nasty Adware. See Figure 2 – 3 CNET® Download Step 2.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

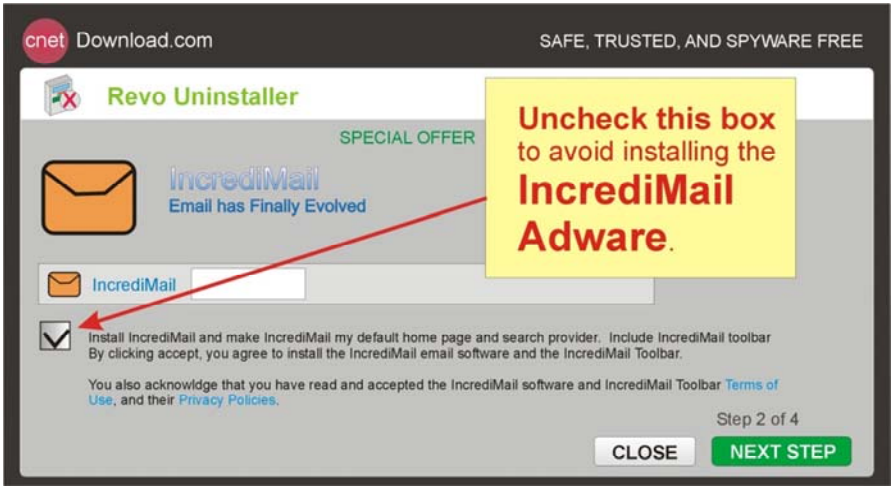


Figure 2 - 3 CNET® Download Step 2

This Windows installs the nasty Adware. Be sure to **uncheck** the install box and any other install boxes as indicated to prevent installation of the nasty Adware. Also make note of the Adware requesting installation. If you ever see it on any computer, be sure to uninstall it. Now click on the green "Next Step" button to continue.

The CNET® downloader program should now skip to the last step as shown in Figure 2 – 4 CNET® Download Step 4. It should bypass Step 3 that downloads the nasty Adware.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

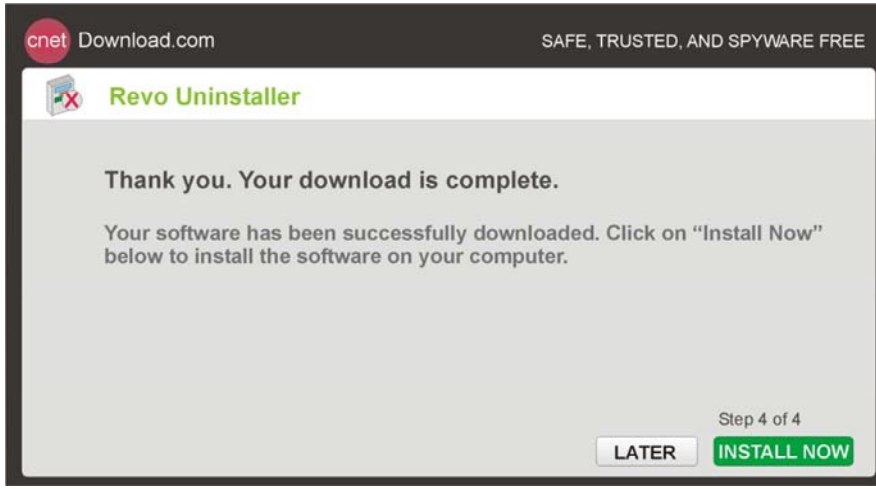


Figure 2 - 4 CNET® Download Step 4

Clicking on the green "Install Now" button should start the installation of the requested software. This avoids installation of the nasty Adware. When I first started this book, this procedure and these precautions were not needed. But with all things that are free, there are advertising strings. It just seems to me that CNET® has gone a bit too far here. An alternate download site is filehippo.com. It can be found at: http://www.filehippo.com/

It still provides direct free software downloads without the nasty Adware installation software.

Another site is FreewareFiles.com. The link to it is: http://www.freewarefiles.com/.

These sites all have search functions that help you locate software. However, they can confuse you purposely into downloading software that you do not want so look carefully for the correct download link – like from a mirror site – after the search has found the software for which you searched.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Nerd Tip: *Read the download page three times before clicking on any download link. Often the link you want is on the side or at the bottom of the page. Labels on links for software that you do not want are most obvious and easy to select by mistake. If you select the incorrect link, you cancel the download and try again.*

Spybot - Search & Destroy

The oldest program is Spybot - Search & Destroy® from Safer-Networking Ltd., a German enterprise. See Figure 2 - 5 Spybot Search & Destroy® Opening Menu. This is a very good tried and true program that is good at catching things that Malwarebytes® does not catch. Sometimes there are difficulties installing it because viruses block it from running or do not permit it to update across the Internet. When it has problems because it cannot get the updates, this can be bypassed by installing without updates. To install without updates requires digging into the menu installation options. When looking at menus please remember to read them several times and then think about what they say. We try to make sure that you always find the correct choice for the frequently used procedures.

While the CNET® editors do not rate Spybot - Search & Destroy® too highly, its user ratings are very good and it has been downloaded over 117 million times. A good way to assess whether a CNET® program is worth trying is to look at the number of downloads and the user ratings. Millions of downloads and good user ratings show that Spybot - Search & Destroy® is a solid and effective virus removal tool. Spybot - Search & Destroy® runs in Safe Mode which is important to us. Spybot works on Vista® and Windows 7® as well.

When first installed Spybot runs through a series of steps that include making a Registry backup, downloading updates, immunizing the computer from infections, and scanning for viruses and malware.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Spybot is free but its author hopes for donations to pay for his time and expenses maintaining the program. If this program helps you, we encourage you to send him a donation.

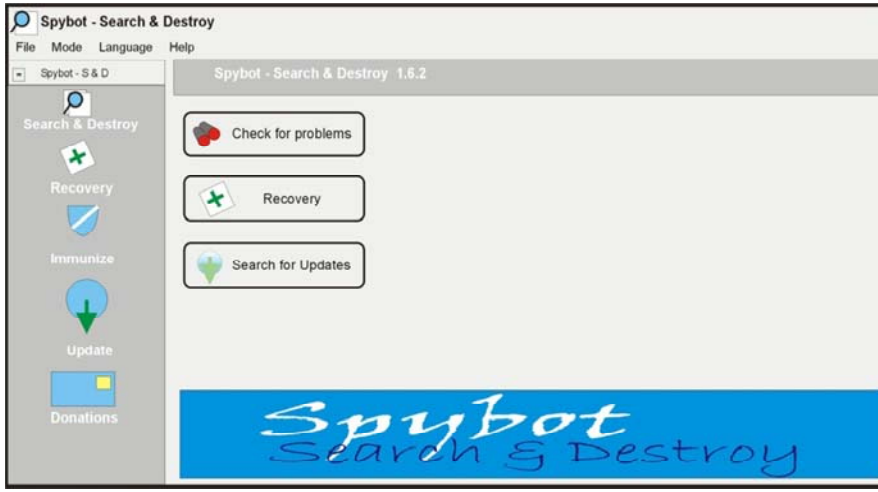


Figure 2 - 5 Spybot Search & Destroy® Opening Menu

Malwarebytes®

This program is the current top virus removal scanning program. See Figure 2 - 6. Malwarebytes® Download. It detects and removes most of the newer viruses. It is so effective that some viruses prevent it from running. Those viruses look for Malwarebytes® by name and block it from running. In that case, you rename the program (the name m.exe often works) so it is no longer blocked. It then runs and removes the virus that blocked it from running. Malwarebytes® runs in "Safe Mode" and works on Vista® and Windows 7®.

If it cannot access the Internet installation errors can occur. In that event, you ignore the errors, complete the installation (when possible), retrieve the updates as an executable program (do a Google® or Bing® search for

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

mbam-rules.EXE file -- the Malwarebytes® offline database installer), and install the rules by running the EXE file.

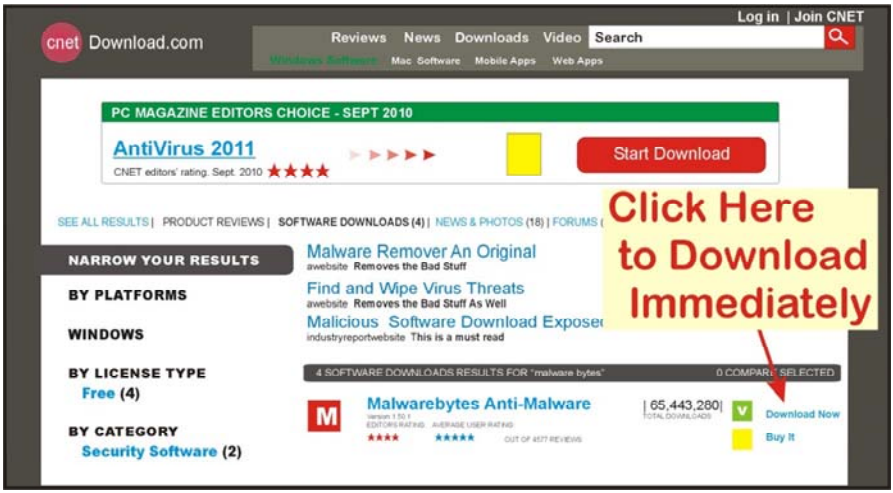


Figure 2 - 6 Malwarebytes® Download

AVG® Antivirus

AVG® stands for Anti-Virus Grisoft®. Grisoft® is the software developer of AVG®. They distribute a free copy for personal use in the hopes that you will buy a licensed copy with more features. Both licensed and free copies are equally effective in finding and removing viruses. AVG® Antivirus can scan a computer in Safe Mode with a command line scan.

AVG® works best in normal mode. So the initial scans are with Malwarebytes® and Spybot Search & Destroy® in Safe Mode. Then the computer is restarted to rerun those same scans in normal mode with AVG® installed.

Many computer users have purchased a security suite of software. A security suite includes antivirus software, spyware software, Internet link scanning software, an enhanced firewall, and other features designed to

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

keep your computer super secure. Often these features duplicate functions provided by Windows®. The duplicated functions are designed to do a better job, but the better job does not necessarily mean better results.

If you already have a Norton® (Symantec®) or a McAfee® security suite that you get for free or have paid for at some time, why would you consider using AVG® to remove your computer's viruses aside from it being free for personal use? There are several reasons. First and foremost, you have a virus in your computer that has compromised Norton® (Symantec®) or McAfee®. So let me ask you, how have those virus protection tools worked for you so far? AVG® is not better but it is equally as good as any other anti-virus program. When installed, it will be a fresh and up-to-date virus removal tool. The key feature of virus removal programs is not scanning for viruses, but rather watching memory to assure that no virus programs begin running while the computer is in use. A good anti-virus memory watcher is critical for preventing and removing viruses.

Virus removal is like pheasant hunting. When hunting pheasants, you use a dog and a shotgun. The dog runs around the field and scares up the pheasants which you quickly shoot with the gun. Hopefully you are a good enough shot to not shoot the dog or any other hunting companions.

With virus removal, Malwarebytes®, Spybot Search & Destroy®, Super Antispyware®, and AVG® all scan for viruses in normal mode. They are the dog that scares up the viruses out of the field (your computer). While those scans run in normal mode with AVG installed, AVG® monitors the computer memory acting like the shotgun. AVG® shoots any viruses that pop into memory as a result of the other program scanning for viruses. This provides a double shot at virus removal.

AVG® is not the only free effective program. Comodo® provides a free antivirus scanner. It has good features but seems a little overly sensitive

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

in detecting viruses. That can be a good thing. If for some reason AVG® does not work, this is a good alternative.

Also the FortiClient® Endpoint Security Standard Edition from Fortinet® works as well. Again use as your selection criteria for picking virus removal tools to download from download.com:

1. Price – free is best,

2. Numbers of user downloads with millions being best, and

3. High user ratings.

The Kaspersky® is good antivirus software and they have some anti-root kit software that is very good. A root kit is a type of virus that loads into the computer's memory as a hardware driver program or from the Master Boot Record. Hardware driver programs make the computer hardware components such as the sound card or the network card function. For all the computer components to function the driver programs are loaded ahead of any other software. They are at the root of the Windows® tree so to speak. The Kaspersky® anti-root kit software may not be free software. The Kaspersky® antivirus is found at a good price in local retail outlets, and on-line. Most virus removal software adequately protects your computer from viruses so there is little need for security suite software. Further, security suite software often slows down your computer and it is redundant with many Windows® functions.

As we said earlier, no anitvirus program alone catches all viruses and spyware. All these programs mentioned here do a good job. Using a full Internet security suite can slow down your computer. It duplicates and enhances (perhaps not for the better) the standard Windows® firewall and security functions. For virus removal only, virus removal programs are needed. Most virus removal programs need to be installed in normal

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Windows® operating mode and not in Safe Mode. Some do run in Safe Mode, but more on this in Chapter 3.

Super Antispyware®

Super Antispyware® is a free program that has a primary focus on Spyware but does a good job removing viruses as well. If you have a nasty virus problem it is good to run this as an added removal step in cleaning up your computer. No matter how many virus removal programs you run, each always finds some missed viruses or spyware.

EASUS® Partition Manager Free

EASEUS® Partition Manager Free is not a virus removal program, but rather a program that permits you to work on hard drive (fixed disk) partitions. It also helps in virus removal by permitting you to rebuild the fixed disk start up information contained in the fixed disk Master Boot Record (MBR). The MBR is the first thing that is read off the fixed disk when Windows® starts. It can be infected by a virus making that virus all but invisible to most virus scanning programs. So part of our procedure uses this program to rebuild the MBR destroying any viruses hiding in it.

Other Tools

Two other tools are from Norton® (Symantec®) and Kaspersky®. These tools are found at the Symantec® and Kaspersky® web sites. They are targeted removal tools and not general purpose virus removers. They go after very specific viruses that are the currently most prevalent viruses.

Nerd Tip: *One way to find a specific program is to use Google® or Bing® to search for that program including the word "download."*

For many years Norton® (Symantec®) has posted specific virus removal tools on its web site. These tools and information on current virus variants are posted at http://www.symantec.com. The Symantec® tool is the

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Norton® Power Eraser or NPE.exe. It can be found by searching Download.com for "norton power eraser". This attacks and removes several of the most active viruses and their variants. It also removes root kits. The root kit removal requires system reboot.

Similarly, Kaspersky® has posted in its removal tools a TDSS root kit removal tool. This tool finds root kits in the Master Boot Record (MBR) that load ahead of any Windows® and virus protection software. Such root kits are hard to detect and remove. The Kaspersky® TDSS removal does a good job of detecting and removing them. Search with Google® for "kaspersky tdss download" to find the tool.

Both tools are found at the Symantec® and the Kaspersky® web sites respectively. However, you must fish around or search vigrously for them.

Summary

This chapter has identified the virus removal tools needed to remove viruses from your computer. It shows that these tools can be downloaded from http://www.download.com and other Internet locations. If your computer cannot access the Internet to download the tools needed, then use another computer and save the installation files on a thumb drive. Once the files are saved, you can then connect the thumb drive into your computer and install the tools.

In Chapter 3 we walk through the procedure to follow using these tools that removes viruses impacting the operation of your computer. Virus removal in several computers is presented along with the strategies needed to remove those viruses encountered. In Chapter 3 repairing the damage done by viruses to Windows® is discussed along with procedures that can restore the computer to normal operation.

Let's move on to Chapter 3 and start killing some viruses.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

CHAPTER 3
Virus Removal Step By Step

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Virus Names

What is in a name? Viruses go by many different names. Here are a few: **emc.exe**, **jkr.exe**, **ulb.exe**, **hfeexe, removewat.exe, ascomenrxw.exe, localeX86.exe**, **GdfsjdvCUN.exe**, **cPdlg02043.exe** called by Registry entry \RunOnce\cpdig02043, **21142919.exe**, **localeX86.exe**, **WINTSVCC32.exe** looks legitimate because it uses common Windows® character sequences e.g. WIN, NT (but not WINT), SVC (but not SVCC), and 32, **Ptipbm.dll**, **Dmonut.dll**, **Itlpfw32.dll**, **ilocaval.dll** called by Registry entry \run\Svohovitogolop, **112A.sys**, **Ctl_w32.sys**, **Mywehit.ini**, **BCBEG.ini** and its inbred cousin **BCBEG.ini2**, **PKP_Dldu.dat**, **Prvlcl.dat**,**1B33.tmp**, and **Kqxjax25212syk721811b172n871yg66c** among others.

My name for them all is G3$D@*7M(&%#@F$#^&*(C!@#S%^&$#$S#@OFAB#$%^. This is a string of words that are best inferred and left unspoken.

Now we can learn several things from virus names. They stand out in a crowd. No self-respecting programmer names his life's most important creation GdfsjdvCUN.exe. Most legitimate programs have an acronymic like name that identifies their function. Just read the C:\Windows and C:\Windows\System32 folders and you understand what I mean. Not in the cards? OK, then just take my word for it.

Some names are random strings of upper and lower case letters, numbers and punctuation symbols. Many are eight characters of less. Many have legitimate extensions like EXE, DLL, DAT, SYS and INI. Some use legitimate Windows® programs like SVCHOST.EXE to load themselves into memory and run. Some of these viruses are loaded in the Windows® Registry using a misleading call. For example, **ilocaval.dll** called by Registry entry \run\Svohovitogolop. This is an attempt by the virus creator to make the true program more difficult to find.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Nerd Tip: *One way to spot viruses is to look at files in several folders under C:\Documents and Settings in Windows® XP and C:\Users in Windows 7® and Vista, and in C:\Windows\system32. If any strange file names like the ones above are spotted, they can be tested by checking the date on the file. A date on or near the date the computer became troubled points to a suspicious file. Selecting the file with the mouse and clicking the right mouse button opens a menu that permits viewing the file properties. Opening the properties link reveals who created the file. Legitimate Windows® programs show that they are copyrighted by Microsoft® or created by Microsoft®. Other programs would show their original creator. Viruses commonly show little or nothing.*

To me it appears that most virus names are created by people living in the Welch town that has the World's longest name. They must have a talent there for creating virus names. If not, where else would virus names be created?

Virus Removal Steps

This Chapter goes step by step through an effective virus removal procedure using the tools identified in Chapter 2. This chapter presents the general procedure. In real life virus removal it is also a good idea to examine the computer's hard drive for virus files and delete temporary files and other files in which viruses hide. This is covered in Step 7 in this chapter.

This is the fun part for Nerds like me so let's jump right in and kill off some viruses.

Installing Virus Removal Tools

When installing virus removal software, there are many choices to make. This is sometimes confusing, if you have not installed that specific software once before.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Nerd Tip: *One simple installation principle that you should use as a guide is "defaults work best." This is the "go with the flow" installation procedure. Try not to pick any custom installation options because it is very easy to make a mistake and have the program not run as required.*

What this means is that you typically answered "yes" to the questions asked and select "next" when prompted. It is also a very good idea to read the menu choices and installation messages closely. It does no harm to read them several times to make sure that you understand exactly what each choice means. Software designers are especially adept at asking questions that are totally confusing to normal people but are perfectly clear to the software designer. The reason for this is that the software designer knows the exact answers he is seeking, while normal people do not. We have no clue where the software designer is trying to lead us.

Please remember that virus removal tools can always be re-configured if they do not operate in a manner that we wish.

Keep in mind our primary goal is running the virus removal software no matter what happens. When virus removal software runs, viruses are removed. Even when virus removing software is not fully updated or configured exactly as desired, virus removal software still removes some viruses. Consequently, when error messages occur we ignore them or bypass them so that the virus removal software starts running. At this point you are beginning a fight to the death with the virus that is messing up your computer. In the battle of virus removal there are no rules. Everything is fair game. It is also socially acceptable to kill any virus, in contrast to killing any human being (which is definitely not socially acceptable).

Basic Procedure

The basic procedure for virus removal when you have only the tools you have downloaded off the Internet has several steps. These steps are:

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Step 1 – Boot into Safe Mode

Virus removal requires a working computer with a working Internet connection. If your computer is extremely slow, then likely viruses or other bad software is probably slowing it down. To gain better control over your computer and remove the viruses, you need to reboot the computer (power it completely off and then restart it) into Windows® "Safe Mode with Networking".

Please boot your computer into Safe Mode with Networking as demonstrated below. Safe Mode with Networking is a special repair Windows® operating mode that loads fewer programs than normal Windows® operation loads into memory.

Windows® with fewer software components loaded into memory looks different than normal. When a computer is operating in Safe Mode the screen typically has a black desktop background, the words "Safe Mode" appear on each corner of the screen, and the desktop icons look abnormally large because the display resolution is set to low resolution (640 by 480 or 800 by 600).

Safe Mode is entered by tapping the F8 key during the Windows® restart – boot up process. See Figure 3 – 1.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Figure 3 - 1 The F8 Key Location

There is a narrow time slot where Windows® sees the F8 key stroke and displays a menu of boot up options where "Safe Mode with Networking" is the second selection from the top. See Figure 3 – 2 Safe Mode Selections below.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

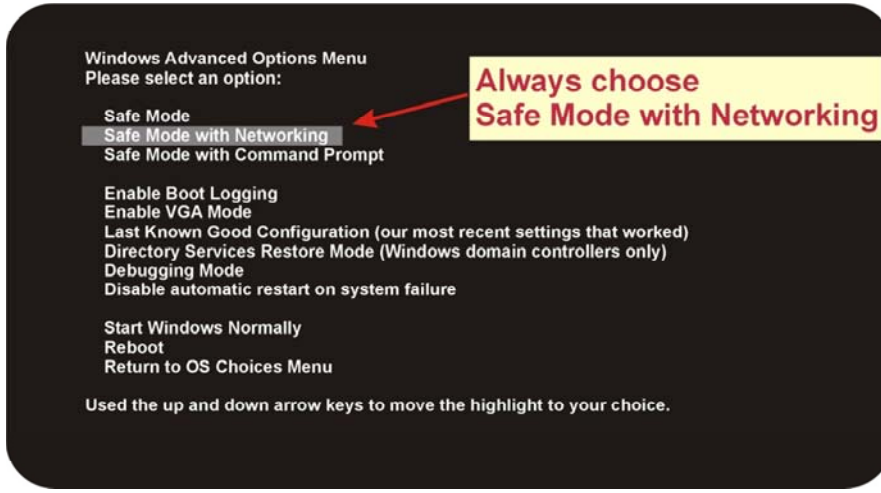


Figure 3 - 2 Safe Mode Selections

After you select Safe Mode, do not be concerned about all the text that Windows® writes to the screen. The text is generally meaningless to computer users and does not indicate added problems with the computer. See Figure 3 – 3 Safe Mode Boot Screen.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Figure 3 - 3 Safe Mode Boot Screen

The only problem that can happen is that the computer is blocked from booting into "Safe Mode". Sometimes you need to wait for several minutes for Windows® to finish booting.

Just prior to the computer booting into Safe Mode, it displays the Safe Mode Warning screen. See Figure 3 – 4 Safe Mode Warning Screen.

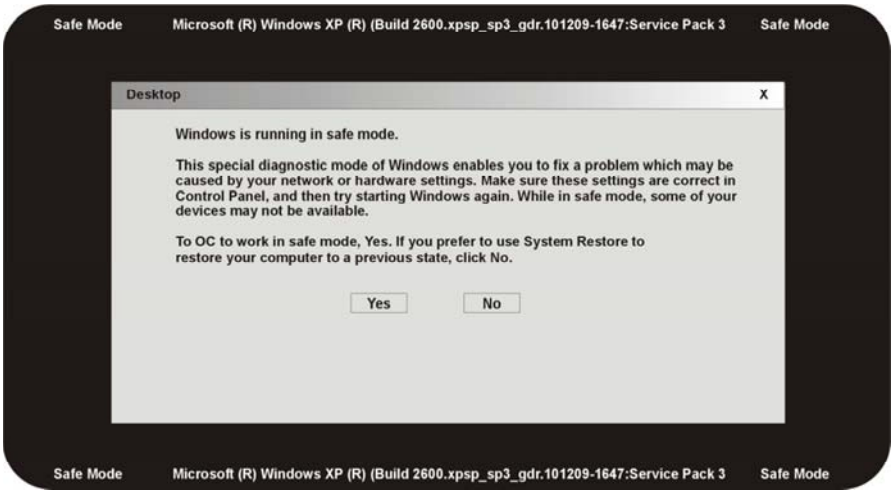


Figure 3 - 4 Safe Mode Warning Screen

If you cannot get your virus infected computer to this starting point, there are other things you can do to complete the repair. One approach requires a separate working computer to download software and to check the sick computer's internal hard (fixed) disk drive. In some cases hard drive removal makes checking easier. Tests to perform on a non-working computer's disk drive installed in another computer are:

CHKDSK /F or CHKDSK /R

Use a virus scanning program to scan the disk drive for virus files

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

The CHKDSK test detects and corrects disk failures that cause Windows® not to start. Do not lose hope, if your computer appears not to run. Windows® can repair the boot setup by installing Windows® over Windows® for Windows XP® or repairing the boot setup with Windows 7® (and Vista®). This is covered in Chapter 6 rebuilding Windows®.

Sometimes viruses make all your data seem to disappear. Do not panic, your data is there. We cover how to find and restore it in Chapter 4. Sometimes no programs run, in Chapter 4 we address that as well so that you can run the virus removal programs.

When you log-in to Windows®, you log into an account. Typically this account is one that was set up when Windows® was initially installed. In Windows XP® this is different from the administrator account. With both Windows 7® and Vista®, the account initially set up can be the only account. As such, it is the administrator account.

When logging into Safe Mode, try to login using the administrator account rather than the user account with which you normally log-in. See Figure 3 – 5 Simulated Safe Mode Login.

This may not be possible with Windows® Vista® or Windows 7®. Using a different account such as the administrator account limits the viruses' ability to block you from running different programs that remove the viruses.

Sometimes you need to create a new account with which to login to the computer. Doing this increases your ability to remove the virus software. A new account may be free to run virus removal software that is blocked from running under the existing user account. When you create a new account, you must make sure that new account has administrator privileges.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Creating a new account is often required when you are removing viruses from a Windows 7® or a Windows® Vista® system. The helpfulness of this new account is illustrated in Chapter 4 as we move through the virus removal process.

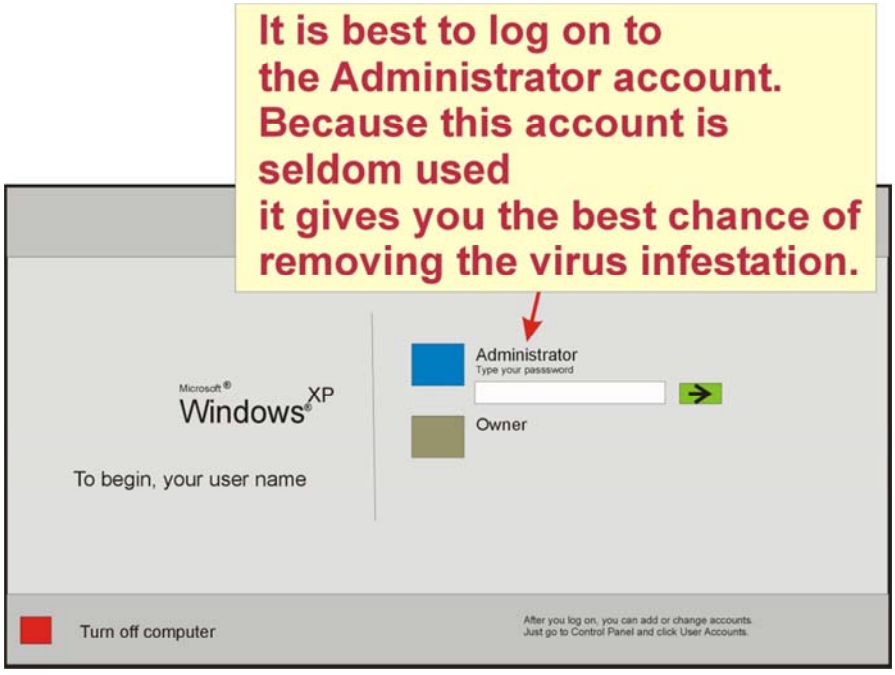


Figure 3 - 5 Simulated Safe Mode Login

The figure above shows logging into an administrative account on a Windows® XP system. The account initially set up with this computer was the account "Pete".

Once login is complete, the Safe Mode desktop shown in Figure 3 – 6 Safe Mode Administrative Desktop appears.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Figure 3 - 6 Safe Mode Administrative Desktop

The Safe Mode desktop looks different from the normal operating desktop. Most noticeable is the difference caused by the VGA display drivers. Safe Mode uses Windows® a low resolution VGA (640 by 480 or 800 by 600) vs. a high resolution XGA (1280X1024) display. What you see is a display where everything is larger than it normally appears on your monitor with the words "Safe Mode" displayed in all four corners of your display. The desktop background is also black.

In Windows® Safe Mode with Networking you have the same Windows® start button and task manager controls that are provided in Windows® normal operating mode. Most all Windows® programs work the same as they do in normal operating mode. Some programs may function differently. All programs look different because of the lower display resolution.

In Safe Mode your computer runs faster because it is not running as many programs as it runs normally. This also means that there is a good chance some of the viruses are not loaded into memory as well. This provides us with the best opportunity to attack and remove them.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Step 2 – Download, Install and Run Malwarebytes®

Our goal now is to remove as many viruses as we can so that we can regain control of the computer in normal operating mode. The next step to accomplish this is to install and run Malwarebytes®. Malwarebytes® is good at detecting and removing many of the newer viruses that attack computers. Malwarebytes® runs in Safe Mode. It is easy to install. Once Malwarebytes® is installed and updated, you perform the full scan. See Figure 3 – 7 Malwarebytes® Full Scan Selection.

Figure 3 - 7 Malwarebytes® Full Scan Selection

Sometimes viruses block installation of Malwarebytes®. The installation program for Malwarebytes® may not run, or maybe blocked from doing updates on the Internet.

When Malwarebytes® cannot run, it is often because viruses look for the name Malwarebytes® (mbam.exe) or the name of the executable program that installs Malwarebytes® (mbam-setup-1.50.1.1800.exe). The solution here is to simply rename the program so that the viruses do not see it

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

load into memory and run. A name like m.exe or a.exe in place of mbam.exe often works.

In the second case, Malwarebytes® is effective in removing viruses and spyware even if it is not updated. So the simplest approach is to simply ignore all error messages and attempt to run Malwarebytes®.

There is also a way to download the Malwarebytes® updates as an EXE file. The link for this file can be found in the forum postings at the Malwarebytes® (http://www.malwarebytes.org) website. Using Google® or Bing® to search for download mbam-rules.exe or for offline database update can also lead you to the download link.

Step 3 – Download, Install and Run Spybot Search & Destroy®

After Malwarebytes® begins to run, you may immediately download, install and run Spybot Search & Destroy®. Windows® is capable of running both Malwarebytes® and Spybot Search & Destroy® simultaneously. These two programs do not appear to interfere with each other when run simultaneously. By running simultaneously the initial job of virus removal finishes in less time than if you were to run first Malwarebytes® and then Spybot Search & Destroy®.

Generally, Spybot Search & Destroy® installs without incident. However, occasionally viruses block Spybot Search & Destroy® installation. This is because they do not permit Internet access. Spybot Search & Destroy® when it is first installed uses the Internet to update itself. When this update is blocked, Spybot Search & Destroy® does not install properly. The workaround for this problem is to install Spybot Search & Destroy® without immediately updating the program or the virus definitions. See Figure 3 – 8 Spybot Search & Destroy® Download Updates Immediately Selection.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

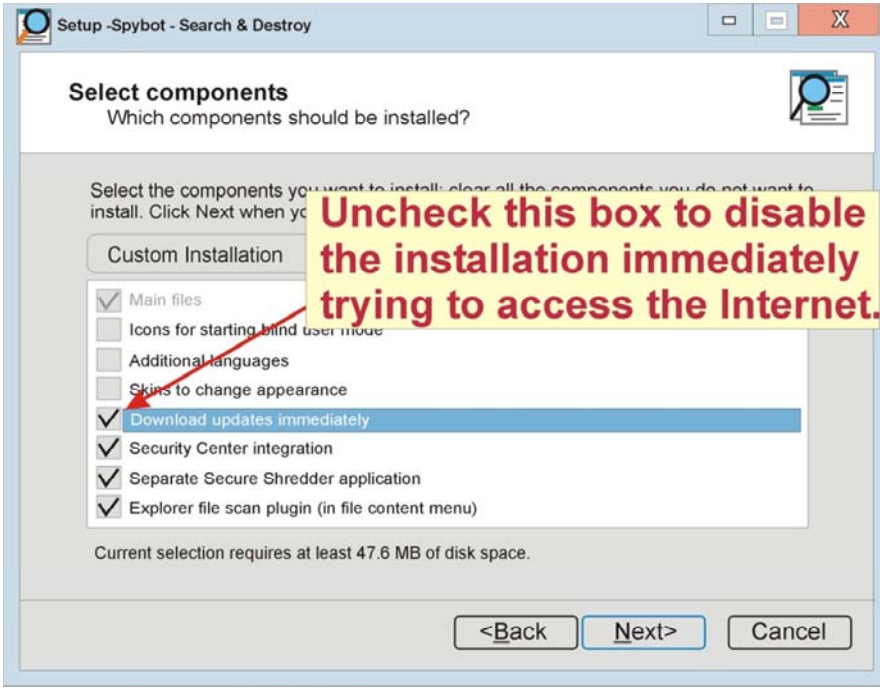


Figure 3 - 8 Spybot Search & Destroy® Download Updates Immediately Selection

When you cannot update Spybot Search & Destroy® to remove the latest viruses, just run it. It is better to run the program with whatever virus removal signature files it has and remove what you can, than to try to update it to get all of the latest viruses. You can always update it to remove all the latest viruses later on in the virus removal process.

Also it is not critical to run the virus removal programs in this exact sequence. If another virus removal program runs and Spybot does not, run it first then re-try to run Spybot.

When Spybot Search & Destroy® is first installed, it walks you through several different steps. Because the computer is already infected with

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

viruses, some of these steps are not necessary. See Figure 3 – 9 Create Registry Backup.

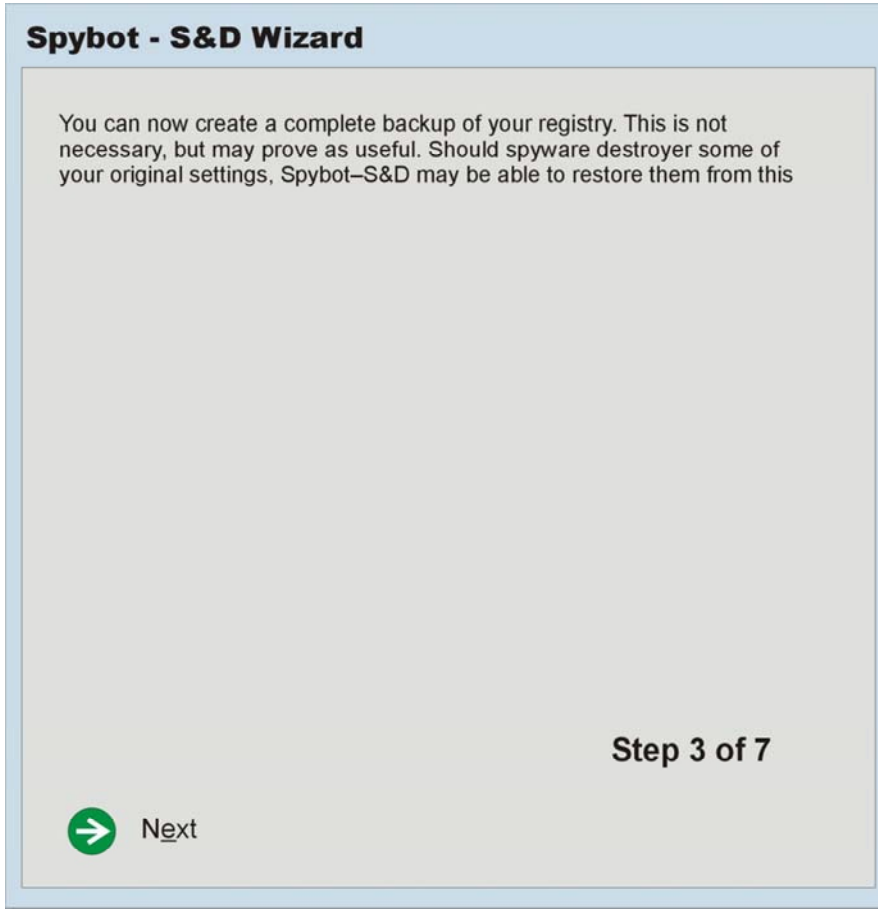


Figure 3 - 9 Create Registry Backup

The Registry backup is unnecessary because the Registry is already infected with virus entries. After the computer is clean and the viruses are removed, then doing a Registry backup makes more sense.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

If you are able to update Spybot Search & Destroy®, the Spybot – S&D Updater window appears. See Figure 3 - 10 Spybot – S&D Updater Window. It is best to pick a download site that is located in the United States. This is because the communications links between sites located in the United States are very high speed communications links, and much faster than communications links connecting to sites that are overseas. The bottom line here is that the files download quicker if you use sites located in the United States.

One of the reasons that the terrorist communications monitoring by the U. S. Government was so effective is because it is cheaper to call the United States from one location in a foreign country and then reroute the call back to a second location in the same foreign country than to call directly from one location to another location in the foreign country. In many foreign countries all communications between the United States and the foreign country are better quality and cheaper than direct point to point communications within the foreign country. When communications were routed through the United States, it permitted the U. S. Government to monitor those communications for terrorist information and better protect everyone worldwide.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

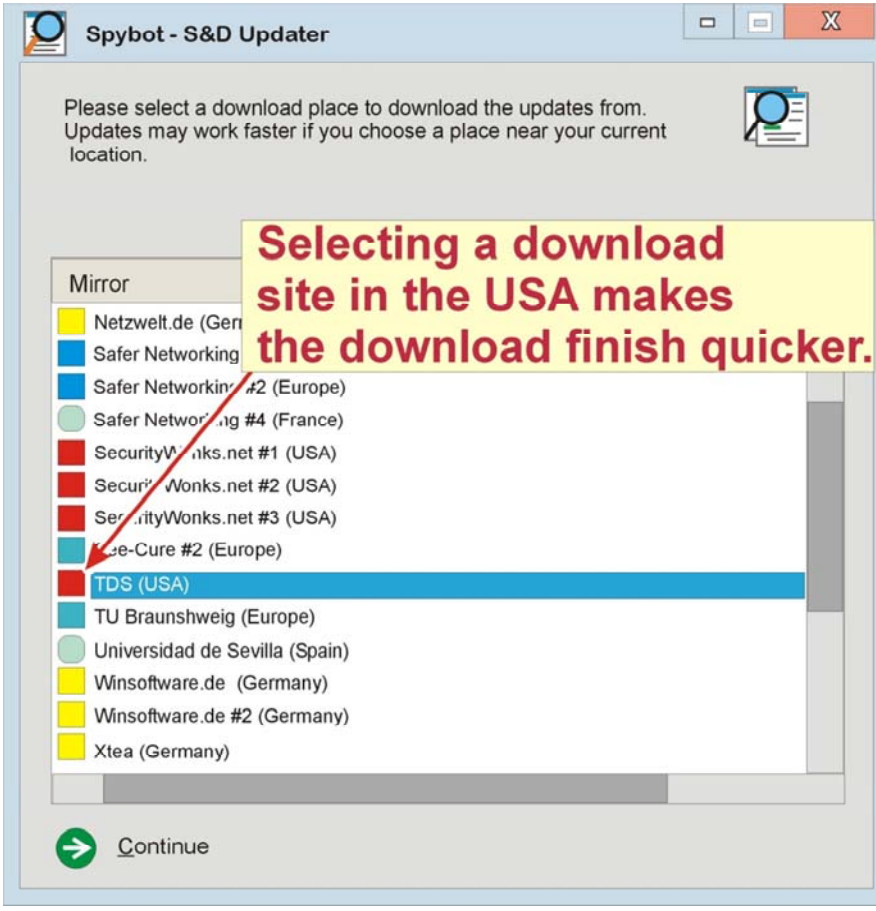


Figure 3 - 10 Spybot - S&D Updater Window

After the S&D Updater compares the install virus definition files to the files at the update site, a list of updates appears. See Figure 3 – 11 Spybot Updates List. To complete the updates you must select every item on the list by checking the box on the left, then click on the download arrow at the bottom. Spybot then downloads and updates its files.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

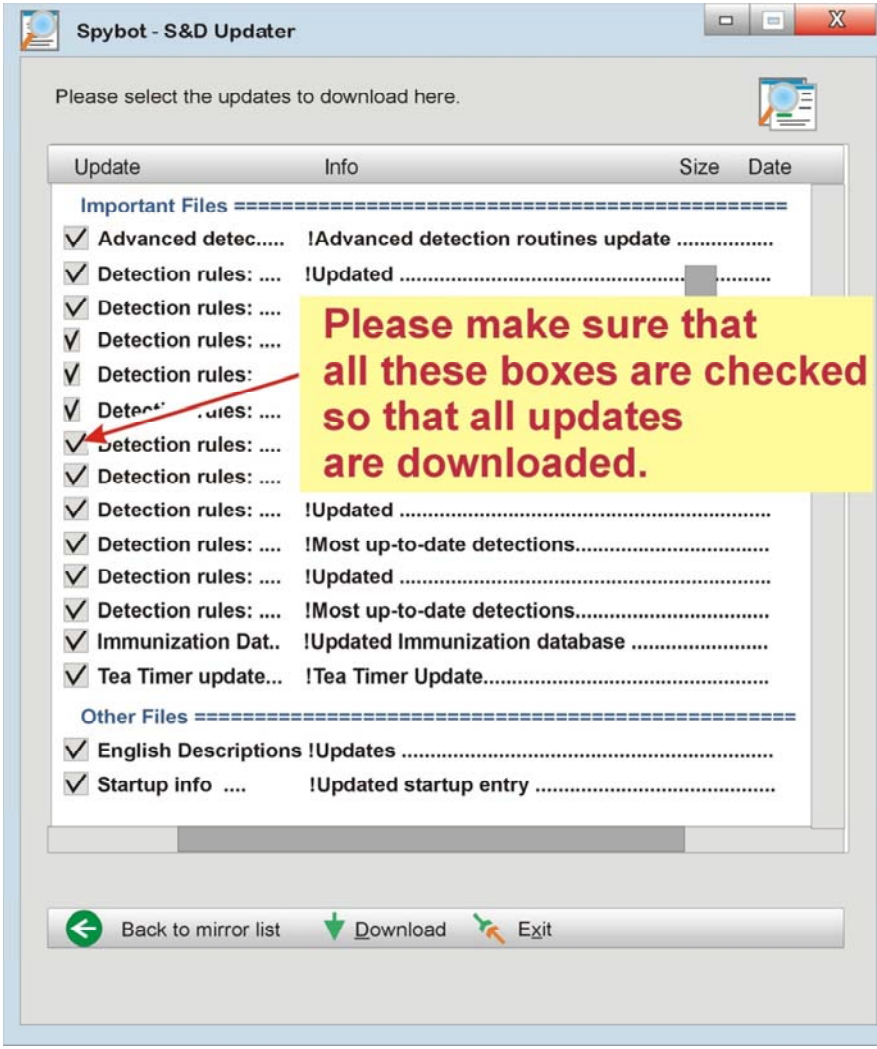


Figure 3 - 11 Spybot Updates List

After Spybot is updated, exit the update program and proceed to run Spybot.

See Figure 3 - 12 Running Spybot. Spybot is launched by clicking on the "Check for problems" button.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

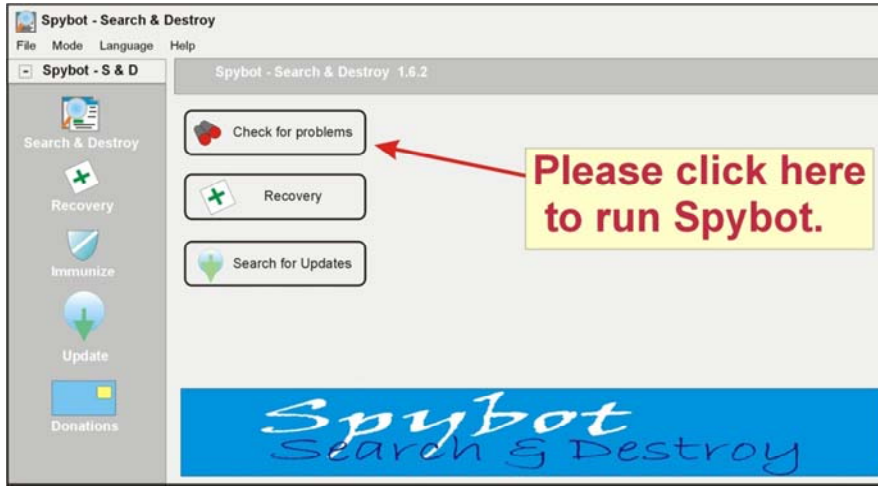


Figure 3 - 12 Running Spybot

As shown in Figure 3 - 13 Spybot Virus Search, when Spybot runs a "Running bot–check" tally is displayed at the lower left of the Window. This tally displays the number of items checked versus the total items to be checked. In the main panel whatever viruses are found are listed. Once the check is complete, Spybot presents a "Fix selected problems" menu option that removes whatever it finds.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

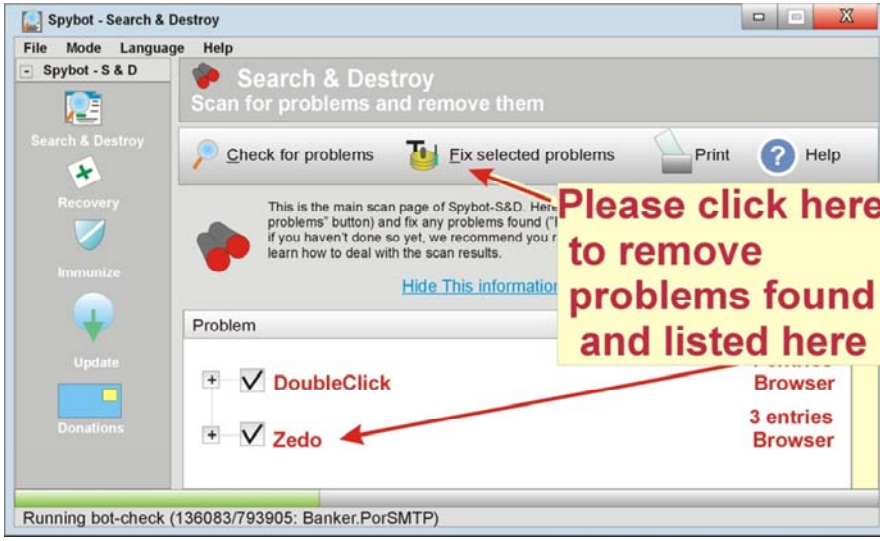


Figure 3 - 13 Spybot Virus Search

Problems found in the search are listed in the Problem ------ Kind panel in red. In this case two sets of cookies were found by the scan so far.

Step 4 – Download and Run Super Antispyware

This is an optional step. The final program you might run as part of your initial virus removal procedure is SUPERAntispyware®. This virus removal program is readily downloaded from download.com. The installation steps are easy to follow and will lead you to the panel shown in Figure 3 – 14 SUPERAntispyware®. Please be sure that the software is updated and then click on Scan Your Computer.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

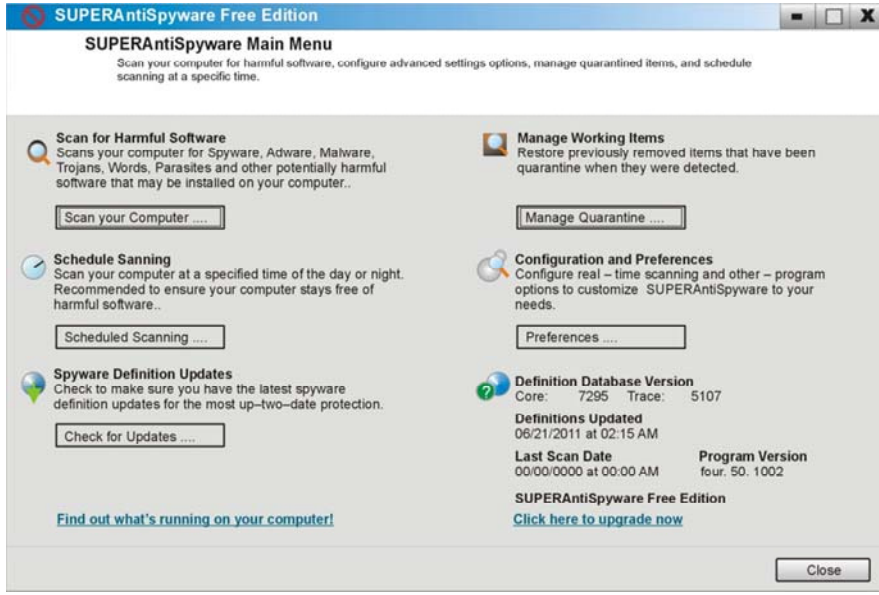


Figure 3 - 14 SUPERAntispyware®

This opens the scanning panel as shown in Figure 3 – 15 SUPERAntispyware® Scan Options. Choose the Perform Complete Scan option as shown in Figure 3 – 15. All the disk drives or disk drive partitions in your computer are scanned by selecting them in the Scan Location panel. The critical disk drive for disk partition to scan is the one in which the Windows® folder resides. Commonly that is identified as drive C:.

Regardless of how many virus removal programs are run, each program is likely to find some problem with your computer. Some of these problems are not serious such as cookies that report information to third parties. Other problems are good to identify and document. Such problems are the locations and names of files that are the viruses themselves. Once these virus files are removed from your computer, they no longer create problems. Sometimes there are viruses that make you behave like a dog chasing its tail. In this case there is a very nasty file or Registry entry that the virus scanning programs have not found which re-creates and replaces

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

the files that the virus scanning programs have found. This is why it's important to run multiple virus scanning programs.

Figure 3 - 15 SUPERAntispyware® Scan Options

Step 5 - Rebuild The Master Boot Record

At this point, we can rebuild the Master Boot Record (MBR) to assure that there are no root kit viruses in it. Both Malwarebytes® and Spybot do not effectively detect root kits in the MBR. Rebuilding the MBR destroys any root kits hiding in it.

Our goal here is to make sure when we reboot into normal mode no viruses are in memory controlling our computer. As we regain control of our computer, we can then complete the virus removal process restoring the computer to the state it was in prior to the virus infestation.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Rebuilding the Master Boot Record (MBR) is done with the EASEUS® Partition Manager program as shown in Figure 3 - 16 EASEUS® Partition Manager Rebuild MBR Selection.

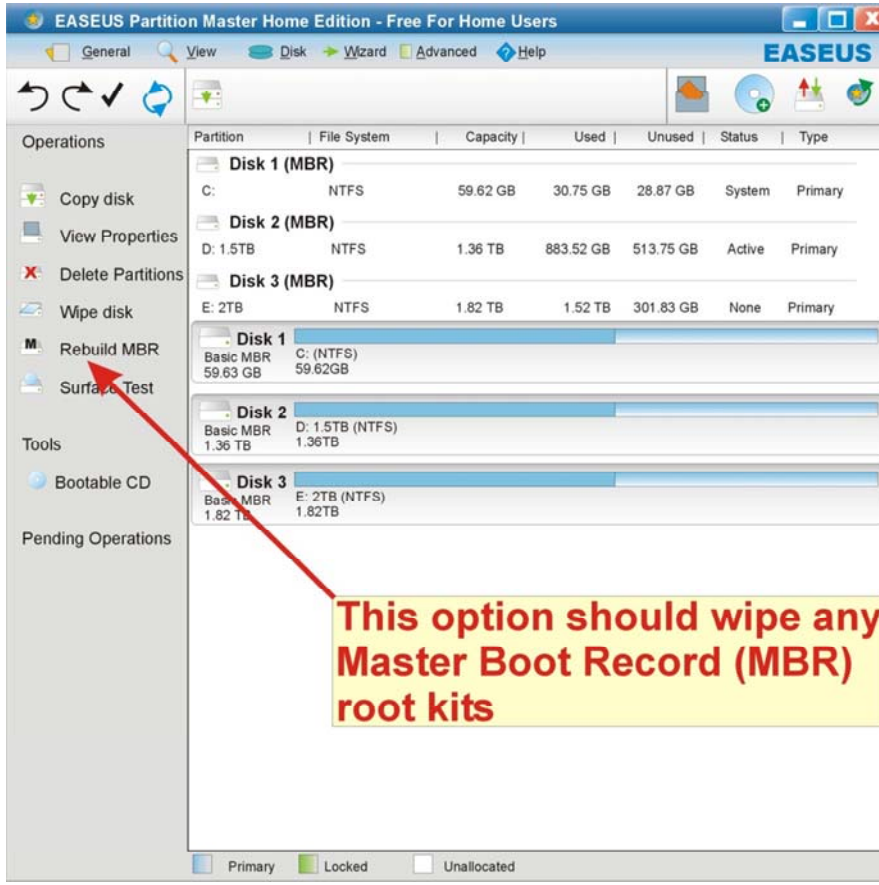


Figure 3 - 16 EASEUS® Partition Manager Rebuild MBR Selection

When the boot disk drive is selected from the EASEUS® menu, a rebuild MBR option is displayed. This rebuilds the Master Boot Record. The rebuild process starts when the check mark is clicked. The check mark is the apply changes option. By requiring you to apply changes EASEUS®

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

forces you to double check your selections ensuring that data residing on your disk drive is not accidentally destroyed.

Step 6 –Complete Safe Mode Virus Removal and Review Results

Let Malwarebytes® and Spybot run to completion. Carefully follow the menus to remove the viruses that they have found, but DO NOT REBOOT THE COMPUTER AS YET. Review the detailed results displayed by both Malwarebytes® and Spybot.

Using the results to identify filenames and file locations can prove to be very helpful and removing viruses from your computer. Virus programs start in your computer by something that opens them. This is typically a registry entry. The registry entry must call a specific file. When the file is completely removed from your computer, the virus program can no longer start and do its damage. Checking to see that the files identified by Spybot and Malwarebytes® have been removed prior to restarting the computer assures that the viruses can no longer impact your computer's operation once it is restarted.

Nerd Tip: *Documenting your results can be helpful and useful if the virus problems persist. WordPad can be used to document the virus removal procedure step-by-step. In all versions of Windows® it is possible to capture the active window by holding down the* ***Alt*** *key and tapping the* ***Prnt Scn*** *key. After the image is captured in this manner, it can be pasted into a WordPad document. Notes can be added to the WordPad document to help you remember what was happening and what choices you made when the image was captured. Be sure to save the document.*

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Step 7 – Remove Temporary Files from the Computer

At this point is also good to remove temporary files from the computer. There are cleaning programs that can do this, but I prefer to do it manually so I know the files are removed from certain key areas.

The first area to remove files is in the C:\Windows\temp folder. All the files in this folder can be deleted. Some files may not delete, because they are actively being used by Windows®. These are typically performance logs. When you cannot delete all the files, check the remaining files to see if any of them look like they may be viruses. Files that have the same size and strange names are always suspect. Right click on the filename and select properties from the menu to further examine the file. If a file cannot be removed, just make a note of it and move on.

The next area to check is the user account temporary files and temporary Internet files. Viruses often hide in these areas. Depending upon the version of Windows®, the folders containing these files are in different locations. For Windows XP®, The files are located in the user account folder in the Documents and Settings folder. They are under a hidden Local Settings folder. For Vista® and Windows 7® they reside under the user account folder in the Users folder.

Removing User Account Temp Files with the Command Console

The easiest way to describe how to delete the TEMP files is to use the command console Window. Open this by clicking on START, then in the RUN (or Search programs and files in Windows 7®) entry area type CMD the hit the Enter key. The command Window now opens. Then use the command:

cd C:\Documents and Settings*ACCOUNTNAME* \Local Settings\Temp

In our example it would be: **cd C:\Documents and Settings*pete*\Local Settings\Temp**

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

then enter

dir /a

to verify that there are files to be deleted. Finally enter:

del *.*

to remove the files.

If prompted, answer

Y

to complete deleting the temporary files.

Nerd Tip: *When using command console commands, upper or lower case does not matter. Upper case is used here to help in identifying the folders.*

In Windows 7® the location is under the Users folder. Figure 3 - 17 Windows 7® Command Console Temp File Deletion illustrates the commands that delete temporary files from Pete's user account.

The first command is:

cd C:\Users*ACCOUNTNAME*\AppData\Local\Temp

In our example it would be: **cd C:\Users\Pete\AppData\Local\Temp**

Next in our specific example some .tmp files are listed using the command:

dir v*.tmp /a (dir *.* /a would show all files**)**

The attributes blocking deletion are removed using:

attrib v*.tmp –r –s –h (attrib *.* –r –s –h would change all files**)**

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

In Chapter 4 there is more information on using the **ATTRIB** command.

These files are then deleted using the command:

del v*.tmp (del *.* would delete all files**)**

One file is in use and cannot be deleted as shown in Figure 3 - 17.

This procedure must be repeated for each user account on the computer to remove the user temporary files.

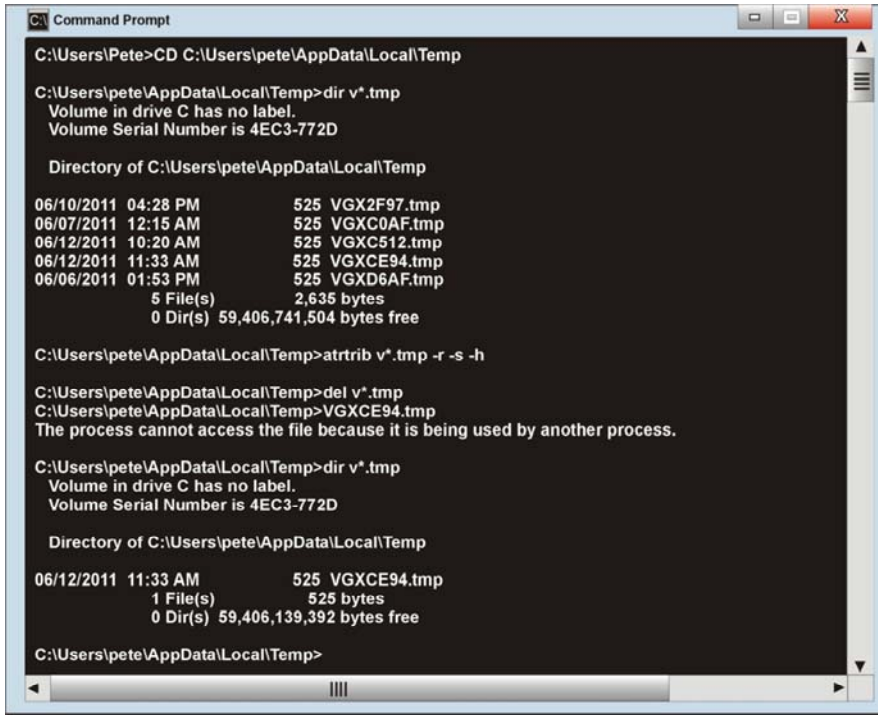


Figure 3 - 17 Windows 7® Command Console Temp File Deletion

For my Windows 7® computer there is only one user account. It is labeled Pete in Figure 3 - 18 Windows 7® User Account Location.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

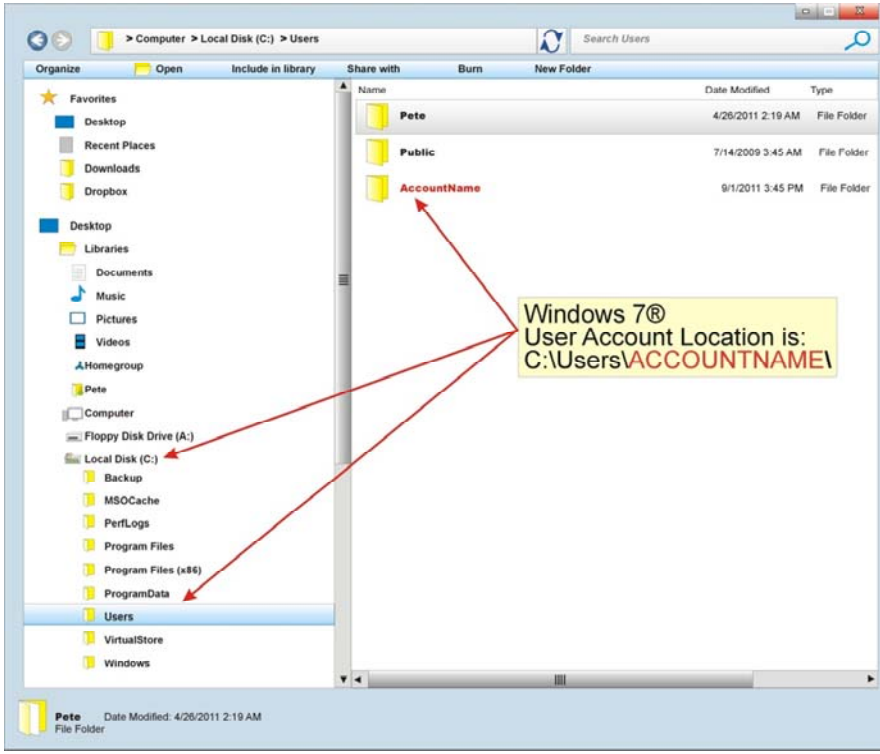


Figure 3 - 18 Windows 7® User Account Location

To find the Temporary Internet Files on a Windows 7® or Vista® computer, we use the command:

cd C:\Users*ACCOUNTNAME*\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5

In our case: **cd C:\Users*pete*\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5**

The Windows® XP command is:

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

cd C:\Documents and Settings*ACCOUNTNAME* \Local Settings\Temporary Internet Files\Content.IE5

In our case: **cd C:\Documents and Settings*pete*\Local Settings\Temporary Internet Files\Content.IE5**

Then use the command: **dir *.* /a**

The DIR *.* /A command reveals the folders containing the temporary files. The files in each folder must be deleted using the exact folder name.

First remove the file attributes blocking deletion for all folders with:

attrib *.* -r -s –h /s

Then delete the files using the command: **del 12345678*.*** for a folder named **12345678**. When Windows® assigns folder names automatically, it commonly uses eight characters (e.g. **12345678**). Windows® often responds with the question: **\12345678*.*, Are you sure (Y/N)?**

Our answer is y or Y to complete the file deletion.

Then verify file deletion using:

dir 12345678*.* /a

Files in use by Windows® and active programs cannot be deleted without special software tools. For the time being we can let these go and plan to come back for them later. Needless to say this process must be repeated for each user account.

Nerd Tip: *The command console command CD works with spaces in the folder name, but DIR and DEL do not. When using DEL or DIR and folders with spaces in their name, the folder name can be shortened to 8 characters by using the first 6 characters in the folder name and then ~1. For example, Temporary Internet Files can be shortened to Tempor~1.*

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

If errors are encountered because of missing folders and files, do not worry about them and just move forward. At any time you wish, you may return to Documents and Settings or Users folder using the CD command e.g. cd C:\users or cd C:\docume~1.

Nerd Tip: *The command console commands can be viewed by typing help at the console prompt. Typing help with the command shows the command structure (Syntax) and command options. For example, HELP DIR displays the Directory command structure and options. Help ATTRIB shows R=Read-only, S=System, and H=Hidden. The + turns the attribute on and the – turns it off.*

The commands shown here should work as typed with the correct folder names. These folder names were the user account folder and the Temporary Internet Files sub-folders.

This is a lot to absorb in a short time period. So relax and try using these commands on another PC. Just avoid removing important Windows files. All temporary files are OK to delete because they are by definition temporary.

Removing User Account Temp Files with the Windows® Explorer

Another way to remove user account temporary files is to use the Windows® Explorer. The Windows® Explorer functions similarly in both Windows® XP and Windows 7®. Launch the Windows® Explorer by clicking on the Windows® Explorer icon in the Accessories folder in Windows XP® as shown in Figure 3 – 19.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

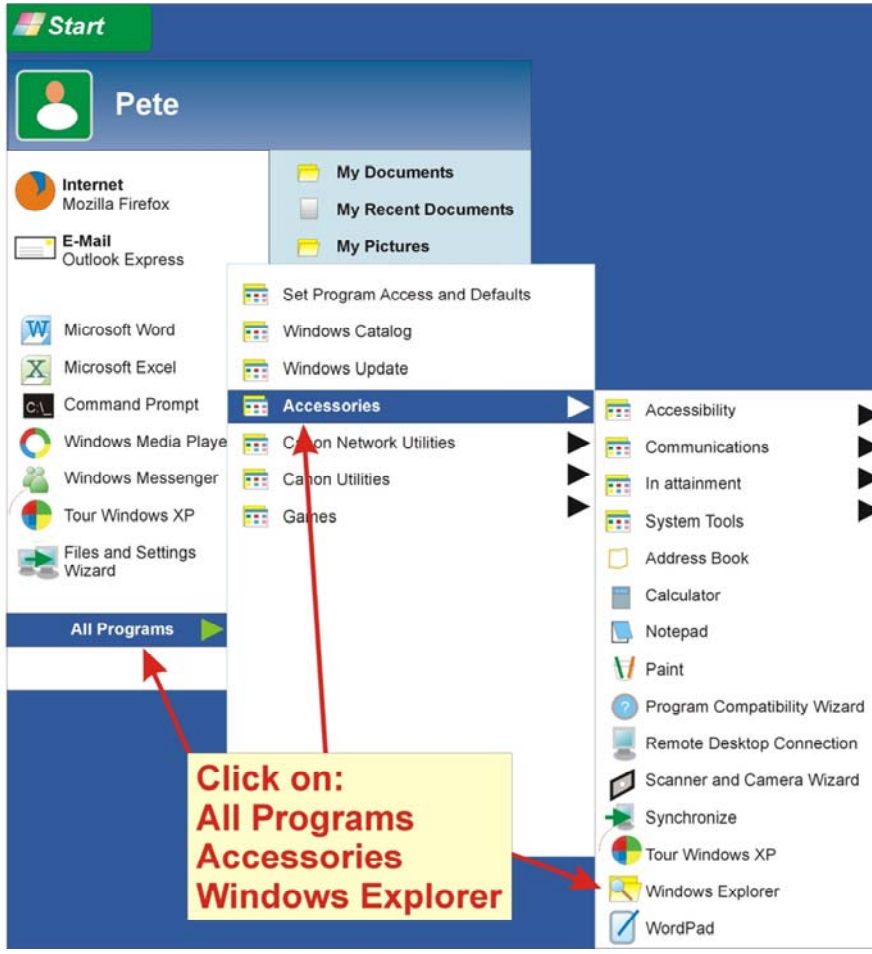


Figure 3 - 19 Windows XP® Windows® Explorer in Accessories Folder

The Windows® Explorer in Windows 7® is pinned to the taskbar. Figure 3 – 20 illustrates this. Clicking on the icon launches the Windows® Explorer.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

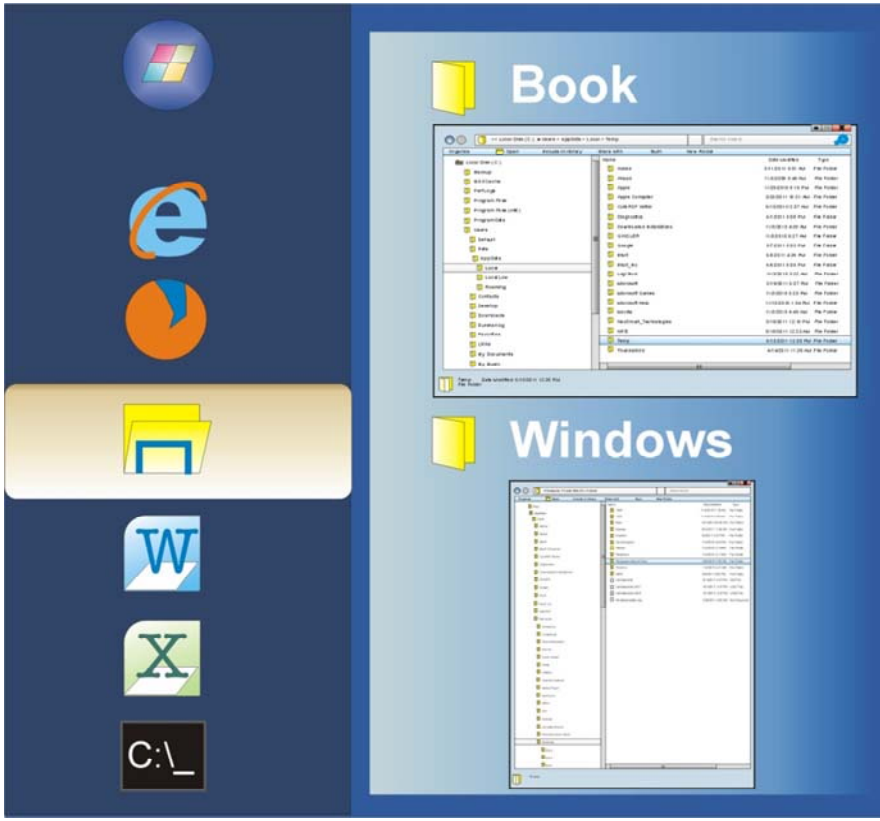


Figure 3 - 20 Windows 7® Windows® Explorer Pinned to Task Bar

In order to remove the temporary files using Windows® Explorer, we configure the view options. The view options are hidden within the Windows® Explorer menus. The locations differ for Windows XP® and Windows 7®.

To find the view options in Windows XP®, we click on the tools option in the Windows® Explorer menus and then select Folder Options as shown in Figure 3 – 21 Windows® Explorer Folder Options Selection. This opens the Windows® Explorer Folder Options menu panel. The View menu is the second tab from the left at the top. Selecting this opens the view options as shown in Figure 3 – 22 Windows® Explorer View Options. In the middle

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

of the menu are the options that change how the system files are viewed. Normally they are hidden as shown in the left panel in Figure 3 – 22. In the left panel all of the "Do Not Show" and "Hide" options are checked. Un-checking these options as shown by the right panel in Figure 3 – 22 causes the Windows® Explorer to display those hidden and system files and folders. When these options are unchecked a warning message is displayed. Just answer yes to the warning message because we need to see the hidden and system files and folders.

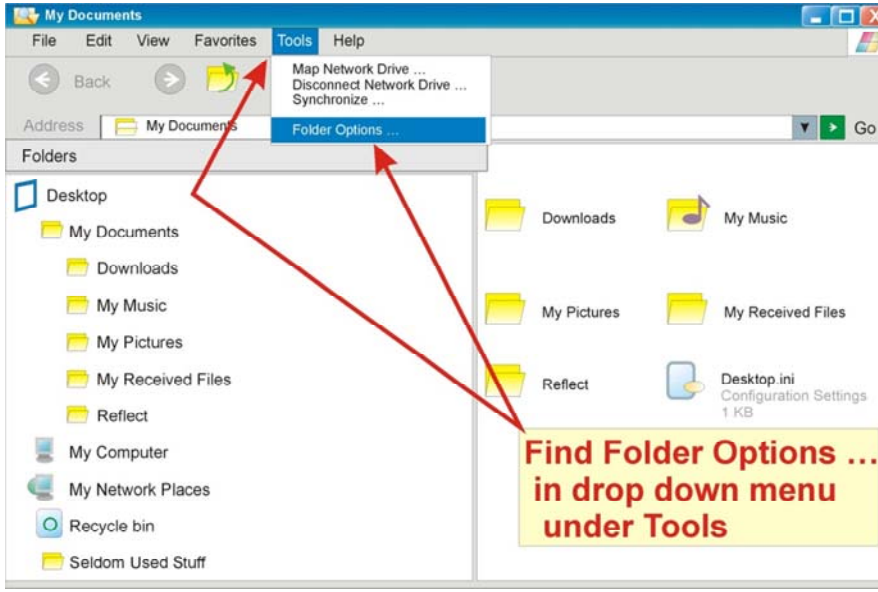


Figure 3 - 21 Windows® Explorer Folder Options Selection

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

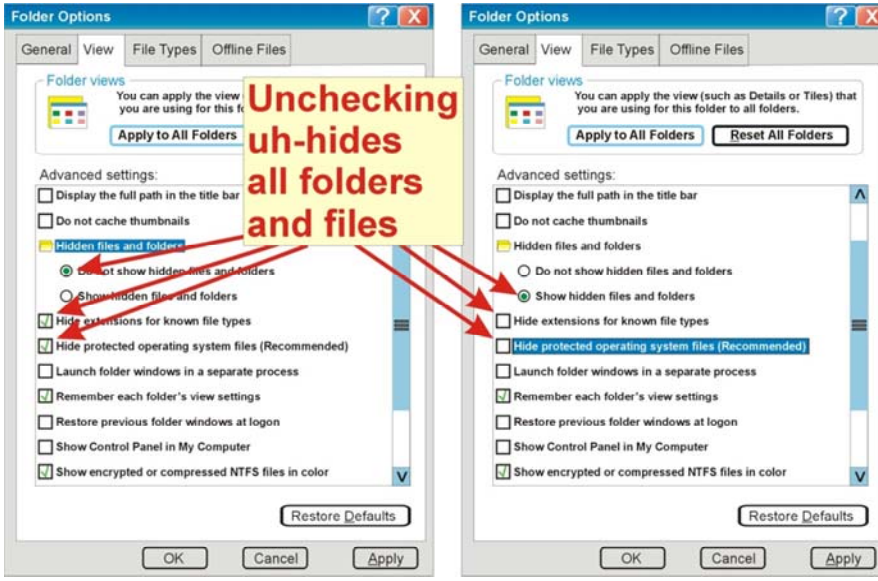


Figure 3 - 22 Windows® Explorer View Options

Although the procedure is similar, the menu locations are different in Windows 7® and Windows® Vista®. The Folders and Search options menu selection are found under the main menu Organize option. When the Windows® Explorer is opened in Windows 7® or Windows Vista®, the Organize option is in the upper left as shown by Figure 3 – 23 Windows 7® Folder and Search Options Location. In Windows 7® the View menu selections are the same as they are for Windows XP®.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

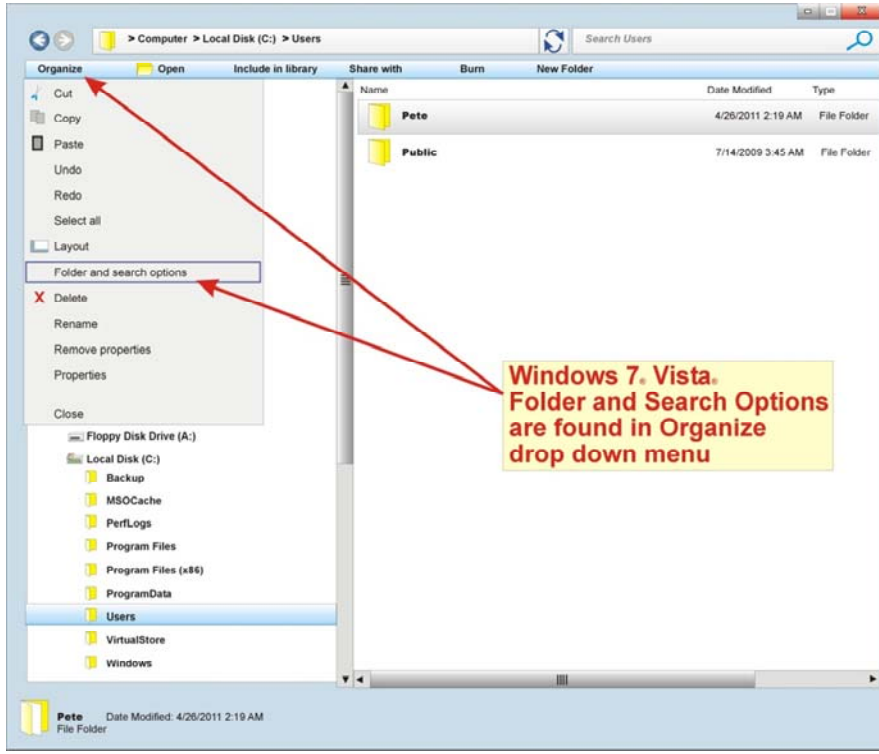


Figure 3 - 23 Windows 7® Folder and Search Options Location

The error message for Windows 7® when you unhide (uncheck) protected operating system files is shown above in Figure 3 – 24 Windows 7® View Change Warning Message. As with Windows XP®, just answer yes to this message so that you can view the hidden and system files and folders.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Figure 3 - 24 Windows 7® View Change Warning Message

The location of the Temp and Temporary Internet Files differs between Windows XP® and Windows 7® as shown in Figures 3 – 25, 3– 26, and 3 – 27. In Windows XP® both the Temp and the Temporary Internet Files are found in the Documents and Settings folder under each user account. To find these files Windows® Explorer must be set to show hidden, and system files.

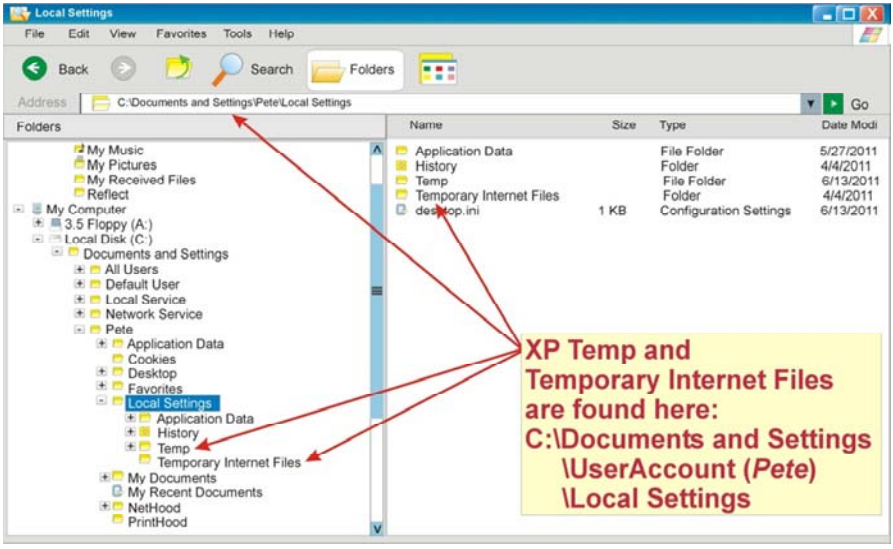


Figure 3 - 25 Windows XP® Location of Temp and Temporary Internet Files

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

As shown in Figure 3 – 25 in Windows XP® these folders are located in the Local Settings folder. The locations are C:\Documents and Settings*ACCOUNTNAME*\Temp and C:\Documents and Settings*ACCOUNTNAME*\Temporary Internet Files\content.ie5. The account name in the example is Pete.

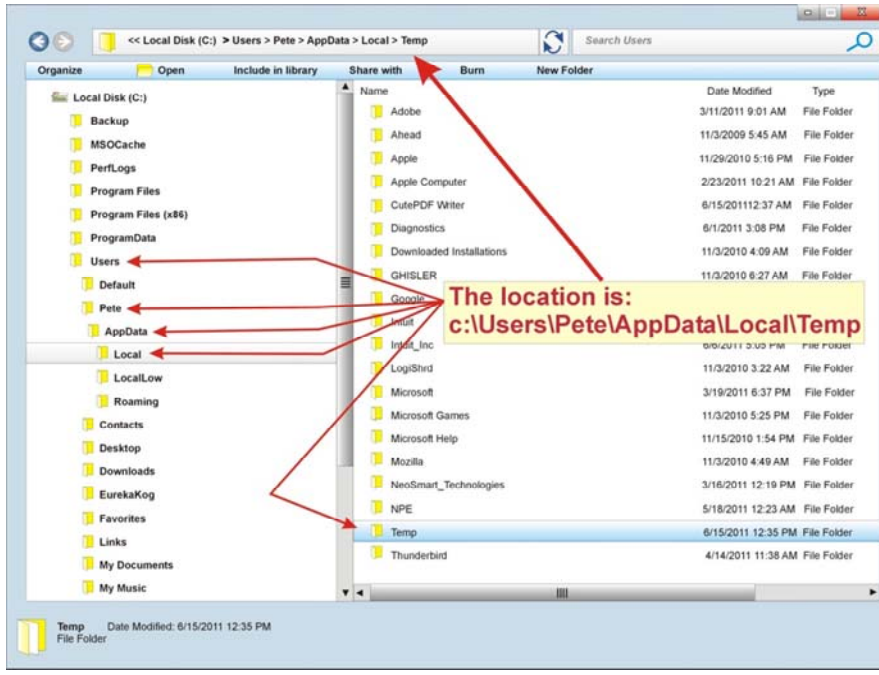


Figure 3 - 26 Windows 7® Location of Temp Files

The equivalent folder in Windows 7® is the hidden folder AppData. Underneath it is Local\Temp for the temporary files. This is shown in Figure 3 – 26 as C:\Users\ACCOUNTNAME\AppData\Local\Temp.

Figure 3 – 27 Windows 7® Temporary Internet Files folder is shown.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

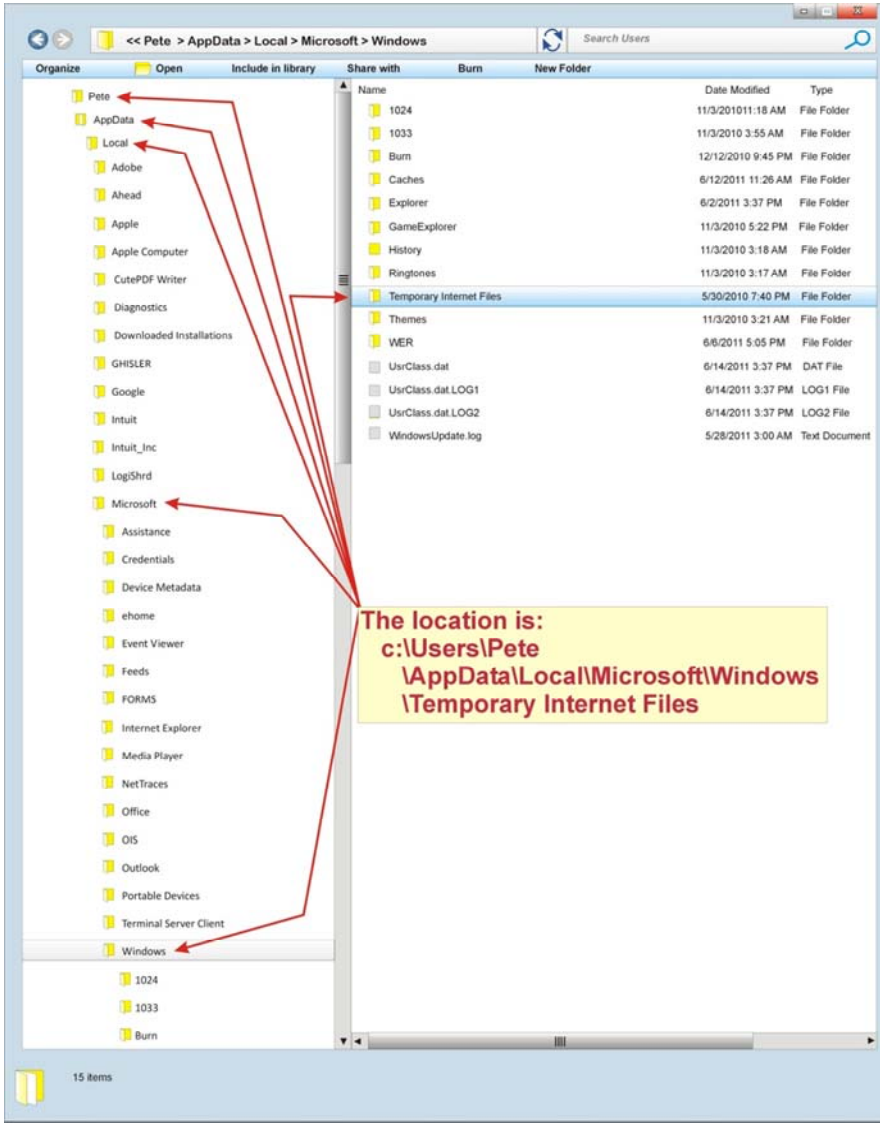


Figure 3 - 27 Windows 7® Location of Temporary Internet Files

To find it in Figure 3-27 you must dig deeper in the AppData folder by selecting the Microsoft® and then the Windows® folders under the hidden folder Local.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

The Windows 7® folder locations are: C:\Users*ACCOUNTNAME*\AppData\Local\Temp and C:\Users*ACCOUNTNAME*\AppData\Local\Microsoft\Windows\Temporary Internet Files\content.ie5 respectively.

In the above example the locations are: **C:\Users\Pete\AppData\Local\Temp** and **C:\Users\Pete\AppData\Local\Microsoft\Windows\Temporary Internet Files\content.ie5**.

Once these folders are located you can use Windows® Explorer to delete all files within them. Such temporary files are where viruses often hide. Sometimes they set themselves up as Hidden and Read-only to avoid detection and deletion. Other times the files are linked to active memory resident programs and cannot be deleted until those programs are no longer in computer memory.

When a file cannot be deleted, point to it with the Windows® Explorer, click the right mouse button, and select properties at the bottom of the pop-up menu. In the Windows 7® Professional and Ultimate versions the file security can be reset by clicking on the security tab, then editing the group or user names, and adding the group everyone with no security restrictions. Figure 3 – 28 Windows® File Properties shows the file properties panel with the security tab selected.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

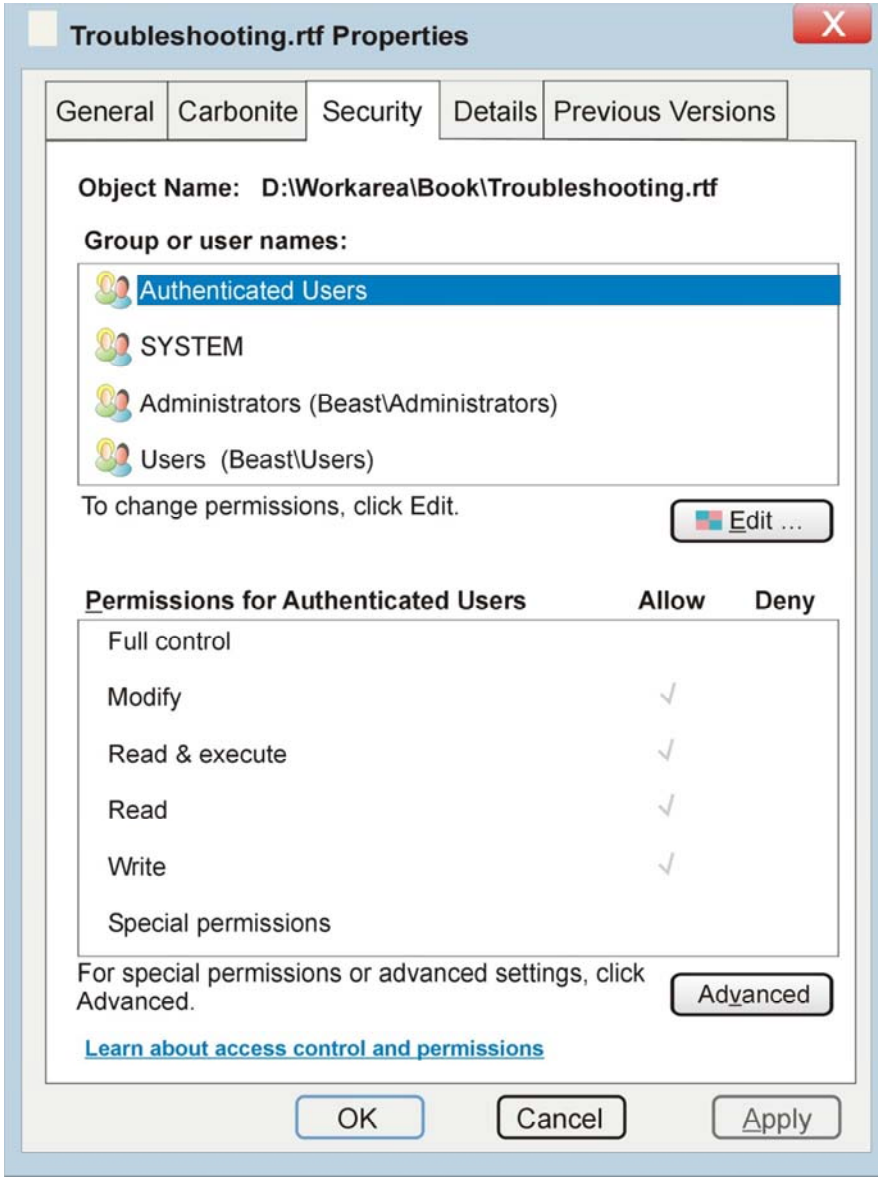


Figure 3 - 28 Windows® File Properties

Clicking on the **Edit** button opens the security permissions panel as shown in Figure 3 – 29 Windows® Security Permissions. Clicking on the **Add**

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

button opens the **Select Users or Groups** panel as shown in Figure 3 – 30 Select Users or Groups. When you type everyone into the **Enter the object names to select** entry area and click on the OK button the group everyone appears in the Windows® security permissions panel as shown in Figure 3 – 31 Windows® Security Permissions with Group Everyone.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

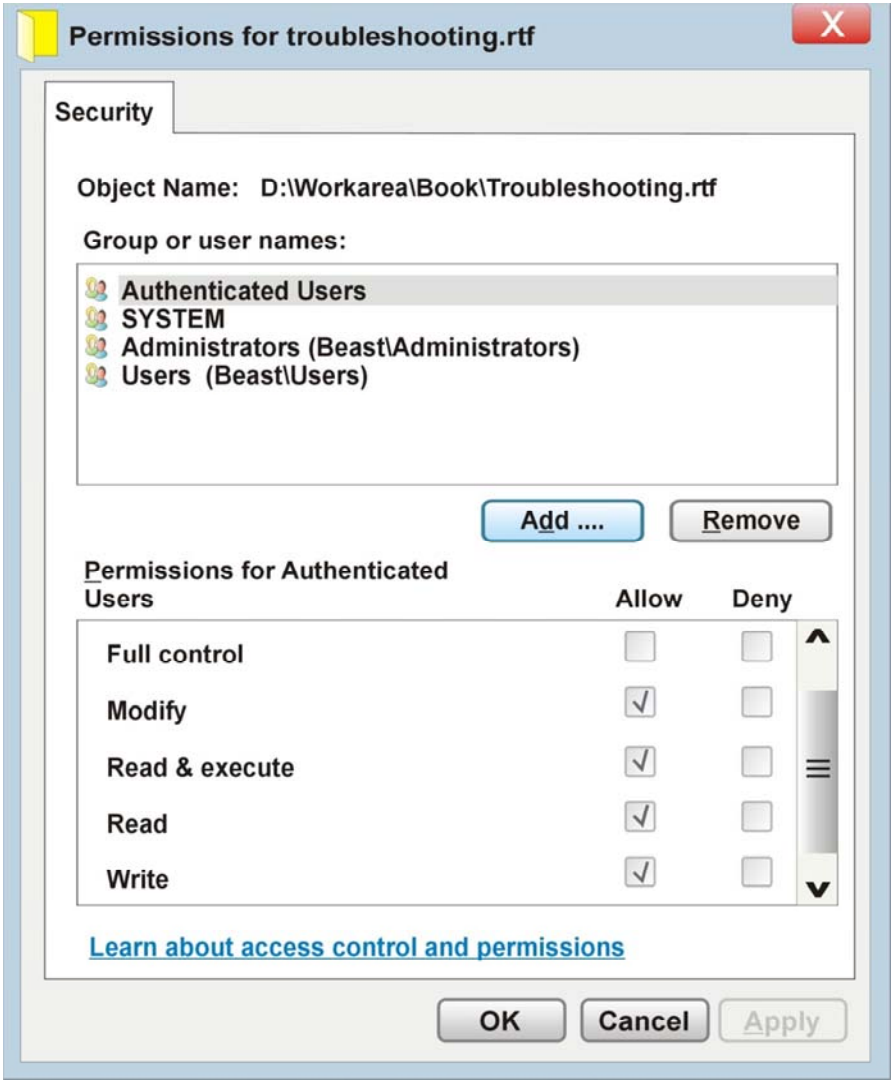


Figure 3 - 29 Windows® Security Permissions

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

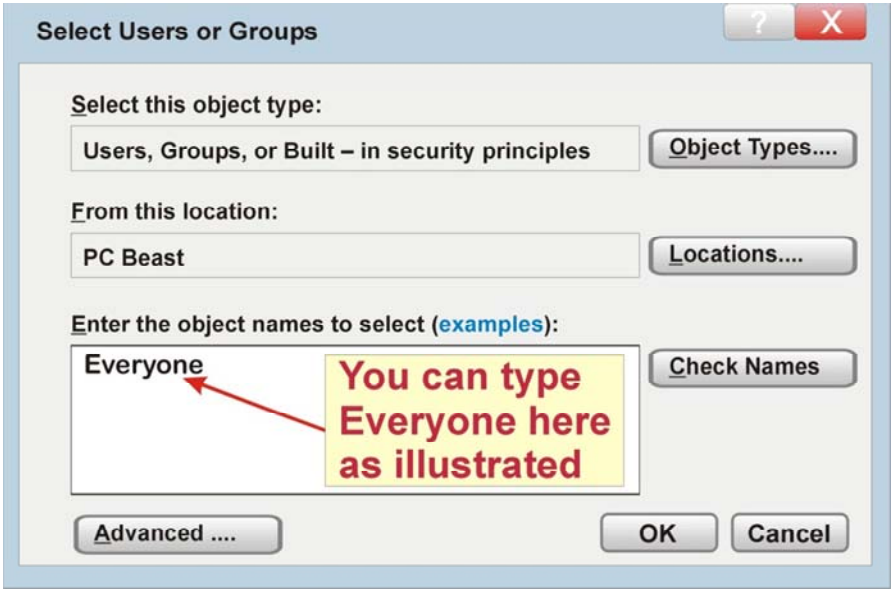


Figure 3 - 30 Select Users or Groups

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

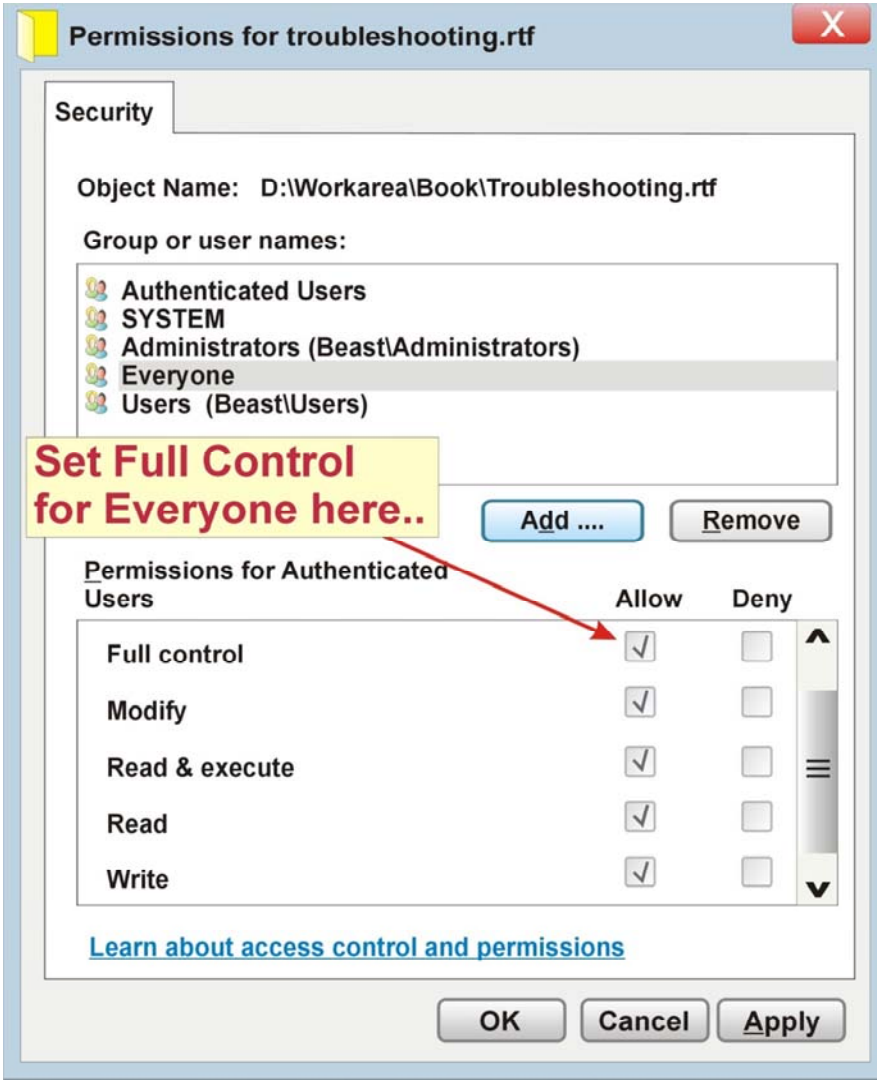


Figure 3 - 31 Windows® Security Permissions with Group Everyone

Checking the box labeled **Full control** now grants full control of the file to the group everyone. Clicking on OK and returning to the Windows® Explorer should permit deleting the file.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

If a file still cannot be deleted, it may be associated with a process that's running in Windows® memory. It is sometimes possible to use the task manager to kill off Windows® processes so that the file attached the process in memory can be deleted. There is no risk of harming Windows® by stopping processes that are running in memory. The worst that happens is that you can cause Windows® to shut down and reboot. One of the SVCHOST processes causes Windows® to shut down in 1 minute when it is terminated. Since there are usually four or five of the SVCHOST processes running at any time in Windows®, there is about one chance in five Windows® shuts down and reboots. Other critical Windows® processes cannot be terminated at all. So again there is little risk of damaging Windows®. When Windows® is rebooted; all the processes are restarted automatically.

Step 8 – Reboot and Repeat Step 2, Step 3, and Step 7 in Normal Mode

At this point it may seem that we have completed our virus removal procedure. While it is true that the basic virus removal procedure is complete, we still have more work to do. It is now necessary to reboot the computer into normal operating mode, log into our user account, and repeat Step 2, Step3, and Step 7. In other words we need to rerun Malwarebytes®, Spybot Search & Destroy®, and SUPERAntispyware®. Since these programs have already been downloaded and installed on our computer, it is unnecessary to download them again. It is only a matter of rerunning these programs in normal Windows® operating mode.

Scanning for viruses in normal operating mode checks the computer more thoroughly because added driver programs and other ancillary software are loaded and running. The Registry keys are also changed. Malwarebytes®, Spybot Search & Destroy®, and SUPERAntispyware® all use the Registry entries to find viruses and other malicious software. Running them in normal operating mode makes sure that we have not overlooked

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

or missed a virus or malicious program that would immediately come back and re-infect our computer.

To misquote a line from a "Godfather" movie, "Just when you think you are free, they pull you back in." What this means is that we are not finished yet with our basic virus removal procedure.

Step 9 – Repeat for Each User Account

Most Windows® computers have a single user account, often identified as Owner. This is a generic way of setting up the computer to work with all of the people that use it under a single user account. These accounts are assigned folders under Documents and Settings for Windows® XP or under Users for Windows® Vista® and Windows 7®.

Some computers are set up with multiple user accounts. Owners often think that this is a way to provide privacy among family members and some added security. Often these multiple user account computers have passwords assigned to some user accounts. This really provides a false sense of security and privacy as we now demonstrate.

First, it is necessary to make sure you are logged onto a user account that has administrative privileges. If not, in Windows® XP reboot into Safe Mode and log in as the Administrator. The Administrator account typically has no password. For Windows® Vista® and Windows 7®, you need to either crack the password or get the password for an account that has Administrative privileges.

Nerd Tip: *When you do not know a Windows® password, do not try to guess it. There are times I have spent hours trying to guess my own password with no success. Find where you can download a password cracking CD image from the Internet. Download the image, create the CD, and use the CD to crack the password.*

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

After you are logged on with an account that has Administrative privileges, use the Control Panel in the User Accounts option to remove the password from the remaining user accounts on the computer. Once the password is removed, you should be able to log out of this account and then log into any other user account on the computer.

Now repeat Step 8 for each user account. This is important because each user account loads a different combination programs from the other user accounts. That means that viruses are cleared from one user account, they are not necessarily cleared from another user account. We explore how this works in Chapter 4 Virus Aftermath Cleanup.

Step 10 – Check and Restart Your Virus Scanning Software

After performing the previous steps, it is now time to check your virus scanning software. When the virus infected your computer, it likely turned off or disabled your virus scanning software. Open the console program for your virus scanning software to determine if it is up-to-date and all the features are working properly. If not, follow the directions it gives to update the software and return it to its active status.

Often the virus scanning software console can be opened using the icon found in the system tray located in the lower right corner of your computer's screen. When you click the right mouse button, a menu should appear which permits you to open the virus scanning software console. Alternatively, the virus scanning software console can be opened using the programs menu.

When the virus scanning software is damaged so much that it does not start, then the solution is to uninstall it and either re-install it or install an alternative virus scanning software package. Both McAfee and Symantec antivirus software and special uninstall or programs available at their

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

websites which completely remove their consumer antivirus software from your computer.

The McAfee® antivirus removal tool can be found here:

http://download.mcafee.com/products/licensed/cust_support_patches/MCPR.exe.

The Symantec®/Norton® removal tool can be found here:

http://us.norton.com/support/kb/web_view.jsp?wv_type=public_web&docurl=20080710133834EN&ln=en_US

If these links change, you may find them by searching for "McAfee uninstall program" or "Symantec uninstall program" using the Bing.com search site.

Other antivirus software has similar uninstall or programs. For example, AVG® has special uninstaller programs. Using an Internet search engine such as Google® or Bing® should lead you to the special uninstall programs.

Another way to uninstall a defective antivirus program is to use a general-purpose uninstaller program such as REVO® Uninstaller. The REVO® Uninstaller program can be downloaded from download.com as shown in Figure 3 – 32 REVO® Uninstaller Download from Download.com. At the download.com site search for REVO® to find the download link for the REVO® Uninstaller.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

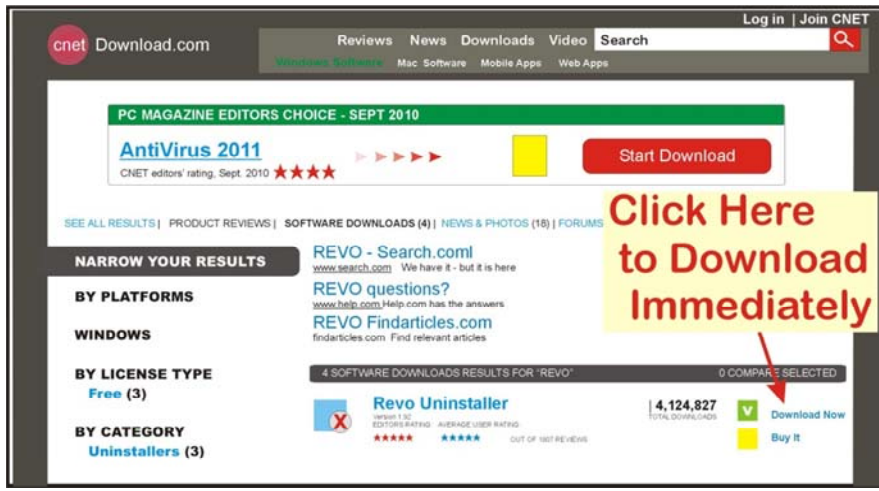


Figure 3 - 32 REVO® Uninstaller Download from Download.com

After the inoperative antivirus software is completely removed from your computer, either reinstall it or install another antivirus software package. AVG® antivirus free edition is an easy to install and is effective antivirus software. Get it at download.com. Simply search for AVG® to find the download link. Be sure to choose the link to AVG Anti-Virus® Free Edition 2011. See Figure 3 - 33 AVG Anti-Virus® Download from Download.com. This link downloads a general-purpose installer program for AVG. During the installation, choose the free basic protection option. There is no need at this time to install a trial version of the full AVG® software package. Other free virus scanning software packages work equally as effective in removing viruses as AVG®. You can find these by searching download.com for "antivirus free". In selecting a package avoid trial versions. These versions are free during the trial, but subsequently request payment when the trial period expires.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

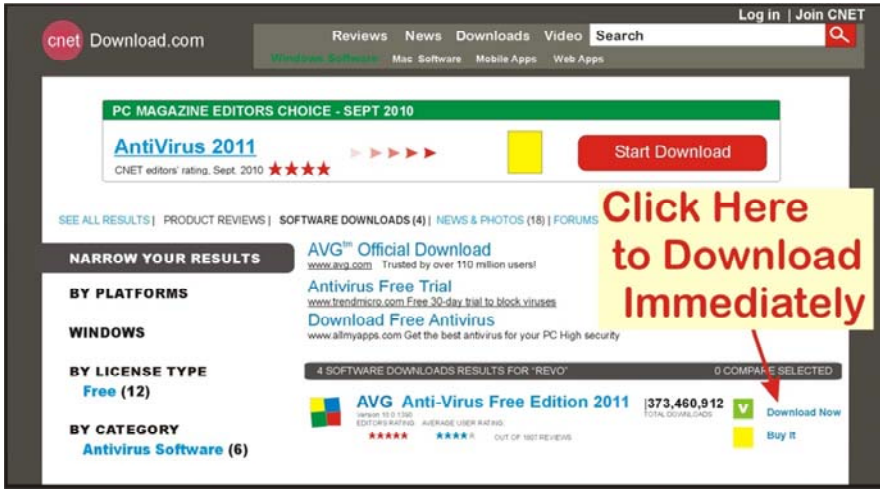


Figure 3 - 33 AVG Anti-Virus Download from Download.com

The best thing about installing a basic antivirus software package is that it does not burden your computer with extra features which tend to compromise the computers performance. Simple antivirus software packages are adequate to protect most all computers.

Once the antivirus software is installed, updated, and running properly, then scan completely your computer for viruses. This is the true final step in the basic virus removal process. All the software that preceded this step is geared to finding the newer viruses by scanning your computer. They are highly effective in completing that task. In contrast virus scanning software is not so much about scanning but more about watching the computers RAM as programs are run to assure that a virus program does not get launched so that it damages or takes over your computer.

Summary

This chapter has described a general step by step procedure for removing viruses from your computer. The detailed step-by-step procedure

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

descriptions presented guide you through this general virus removal process. What is important to remember here is that the details are less important than the overall procedure. Details change often. Please do not get bogged down in details described here. Use them as a guide when you have questions while trying to perform the procedure. So it is best to read this chapter over quickly to get a feel for the procedure. Then as you are actually performing the procedure and you have a question, see if you can find the answer in the step details described in this book.

Nerd Tip: *A very good way to detect and remove the last remnants of any virus is to run Malwarebytes® after your virus scanning software is up-to-date and running properly. This technique of virus removal is like pheasant hunting.*

When you hunt pheasants, a dog and a shotgun are used. The dog runs out in the field and scares up the pheasants. When a pheasant pops up out of the field and tries to fly away, you shoot it with a shotgun. In our case Malwarebytes® is the dog. The virus scanning software is the shotgun. So when Malwarebytes® re-scans the computer examining each file, it brings them into memory where the virus scanning software also examines them and removes them like the shotgun shooting the pheasant when they are a virus. This is a more effective virus removal technique, than scanning alone with Malwarebytes® or with your virus scanning software.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

The general virus removal procedure presented here is:

Step 1 – Boot into Safe Mode

Step 2 – Download and Run Malwarebytes®

Step 3 – Download and Run Spybot Search & Destroy

Step 4 – Rebuild the Master Boot Record (MBR) using EASEUS Partition Manager

Step 5 – Review Results

Step 6 – Remove Temp and Temporary Internet Files

Step 7 – Download and Run SUPERAntispyware

Step 8 – Repeat Step 2, Step 3, and Step 7 in Normal Mode

Step 9 – Repeat Step 8 for All User Accounts

Step 10 – Check and Restart Your Virus Scanning Software

This general procedure should remove most all virus files from your computer. That does not mean however that the job is completely finished. Oftentimes viruses corrupt Windows® itself. In Chapter 3 we address problems that act as impediments to completing the general purpose virus removal procedure described here in Chapter 2. Procedures to resolve these impediments are discussed and examined. These procedures are often necessary to restore Windows® to normal operation after viruses have infected a computer. The longer viruses are allowed to run inside a computer, the more damage they inflict on Windows®.

The Iranian centrifuge destroying virus is a fascinating tale and a great foundation for a nerd spy novel. It was a Windows® born virus that was benign to the Windows® computers carrying it and consequently

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

undetected. The Iranian centrifuges were operated by a commonly used Programmable Logic Controller (PLC) made by the German industrial giant Siemens. They were networked on a network that was not connected to the Internet. So the virus did not travel across the Internet directly to the Iranian computers, but rather hitched a ride on Windows® computers. When the Windows® computers were connected to the Iranian centrifuge network, the virus recognized the Siemens PLCs and infected the centrifuges.

The virus did not immediately do any damage but rather waited until a very specific and exact set of operating conditions were detected before it damaged the centrifuge. In this way it infected more centrifuges and when they were at a specific stage in the Uranium enrichment process then caused their destruction. This is probably the first case of true Cyber Warfare.

Although the Siemens PLCs are used in a myriad of applications Worldwide, the virus only attacked those PLCs in uranium enrichment centrifuges. What a nerd spy story!

The virus that infected the Iranian centrifuges and damaged them is not something that is likely to happen to Windows® computers. It may be possible for a virus to overheat a CPU in some computers (but not all computers), but the computer is likely to power off before this happens. A virus could damage the disk drive by corrupting its contents. However, Windows® viruses want the computer to continue to operate and work in a manner that benefits the virus creator and spreads the virus.

Viruses infecting Windows® computers to my knowledge have not physically damaged those computers. Computers are not uranium enrichment centrifuges. When a Windows® computer is physically damaged it's usually due to a power surge, overheating, poor component design, old-age, hammer damage, or gasoline and a match. After all there

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

is no Windows® computer problem that can't be solved because you can always resort to using a hammer or gasoline and a match. When a computer burns, fire insurance typically pays for a new computer.

What Windows® viruses do is corrupt Windows® and the data on the computers disk drive. A current virus marks the user's data in Documents and Settings or in Users as Read-only, System, and Hidden. Instantly all the computer owner's data disappears. The computer owner cannot see it, but the data is still on the computers disk drive. Such issues are discussed in the next chapter. So it is time now to move on to Chapter 4.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

CHAPTER 4
Virus Mop Up

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Virus Removal Residual Problems

Virus removal is a humbling experience. Once I had a business partner that "knew it all". If you were not sure, you could just ask him and he would tell you that he definitely "knew it all". This led me to the understanding that when you think you know something, you do not really know it. This is particularly true of computers because they change daily.

After having performed virus removals for several years I ran across a particularly nasty one. When the computer was scanned, the virus was found and removed. However, when the final wrap-up scan was performed, then same virus file had reappeared. After repeating the same steps several times with no luck on removing the virus, I at least tried a different approach unlike the current United States President that wishes to just do more of the same ineffective spend, spend, and spend more policies.

When I tried something different, I discovered like Bill Clinton and Dick Morris, that the virus was using triangulation. The virus attack used a combination of three entities, launching entries in the Registry, a file that when launched created the virus file, and finally the virus file itself. So when I performed my standard virus removal approach, it only found the virus file. The computer was immediately re-infected upon restart. Discovering this led me to search further and finally remove the virus.

In the case of Clinton and Morris, they pitted two entities against each other (Left Vs. Right) while they avoided harm to themselves in the middle. This made them look like heroes solving a national problem to both the Left and Right. Unfortunately, the current administration has taken this triangulation to another level and made it multi-dimensional angulation. So there are now 20 different groups fighting each other and

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

nothing gets done in Washington. This is the wisdom of our current crop of politicians at work.

Virus Aftermath Cleanup

Removing viruses from Windows® computers is less of a step-by-step general procedure and more of a thinking how to overcome impediments that occurred during the virus removal process. Virus software throws up all kinds of roadblocks and impediments to prevent removal. Many of these are disguising virus programs themselves with names that may look like normal Windows® files. In other cases random names are generated so that virus removal software cannot search them out by name and remove them easily.

After the viruses are removed following the basic procedure outlined in Chapter2, Windows® may be damaged and require repair. There are four common types of damage that viruses inflict on Windows:

1. They block the Internet Explorer, Fire Fox and other web browsers from connecting to web sites. Web browsers running on Windows® are all interconnected so blocking web site access on one blocks access on all.
2. Sometimes as a defense against removal the viruses block all EXE files from running. In this case you get strange error messages when Windows® launches.
3. Viruses can make it appear that they have erased all your data by using Windows® file and security settings to hide them from you.
4. The viruses corrupt your user account. Usually this is a corruption of the basic configuration data NTUSER.DAT.

In this chapter we show you how to fix these four common problems. The first two problems are caused by bad configuration or Registry entries. The third problem has the security and file attributes changed for all files. The fourth problem is caused by a corrupted NTUSER.DAT user account

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

configuration file. These problems are readily resolved. New viruses may create new problems. Consequently, the intent here is to give you an idea of how to think of things to do that overcome the damage that virus programs do to Windows®.

Often to remove viruses you must like act like a bulldog and never let go or ever give up. It helps to continually ask your-self these questions: "Is there anything else I can do?" or "What else can I try?" For every roadblock you encounter, you need to think of how you can get over, under, around, or through that roadblock. Often this is very frustrating. Please remember that persistence always prevails.

Damage Type 1 – Internet Explorer Cannot View Any Web Sites

One of the most common problems virus infections leave on a computer is blocking Internet Explorer or Firefox from accessing webpages after the viruses are removed. Viruses do this by setting up a proxy server link in both Internet Explorer and Firefox. Because Firefox mirrors the setup of Internet Explorer, when a proxy server link is set up in Internet Explorer, it is also set up and Firefox.

The proxy server setting is easily removed from both Firefox and Internet Explorer. We start by removing it from Internet Explorer. Please open Internet Explorer. In the upper right-hand corner select the tools menu. The drop-down menu for Internet Explorer tools opens. At the bottom of the menu is the Internet Options selection. This is shown in Figure 4 – 1 Internet Options Selection.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

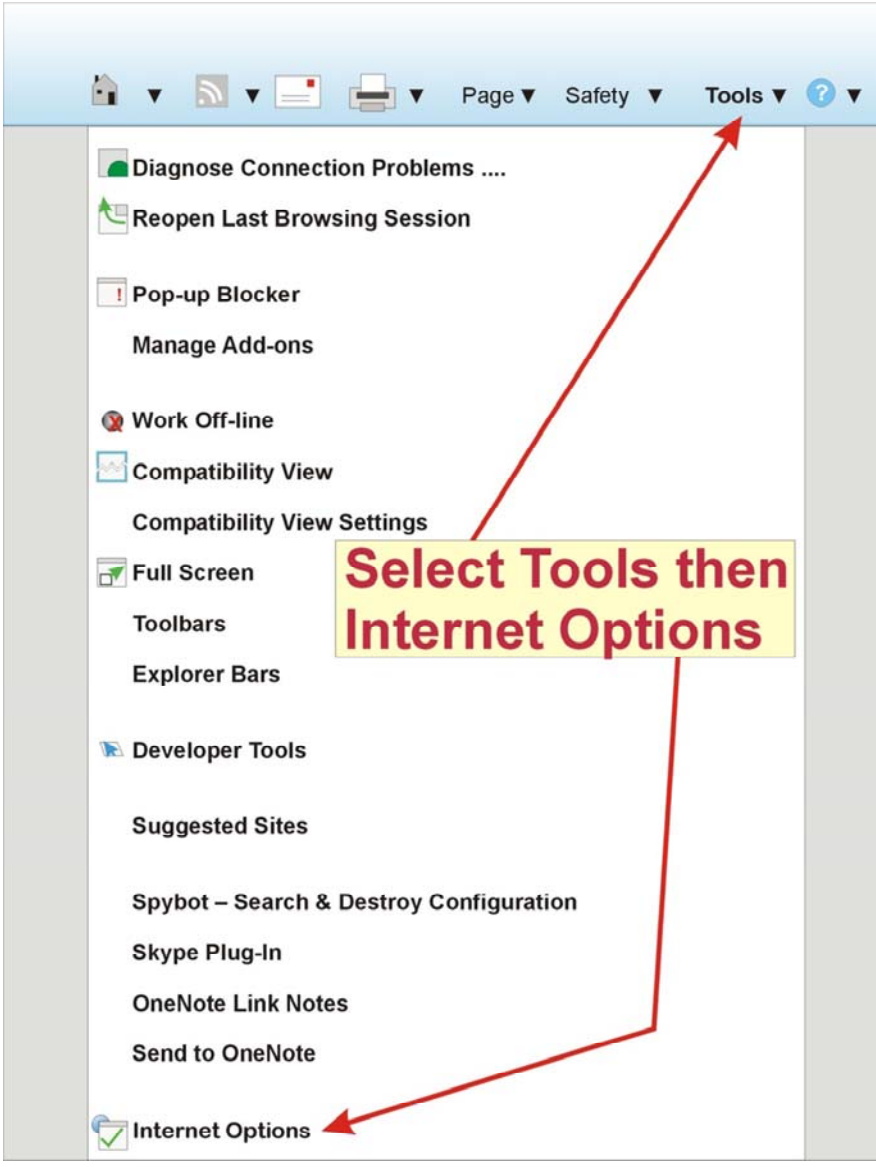


Figure 4 - 1 Internet Options Selection

When the Internet Options menu item is selected, the Internet options panel shown in Figure 4 – 2 Internet Options Panel appears. Please select

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

the **Connections** tab in this panel which will reveal a **LAN Settings** button on the bottom right. Selecting this button leads to the Local Area Network (LAN) Settings panel that controls a proxy server selection.

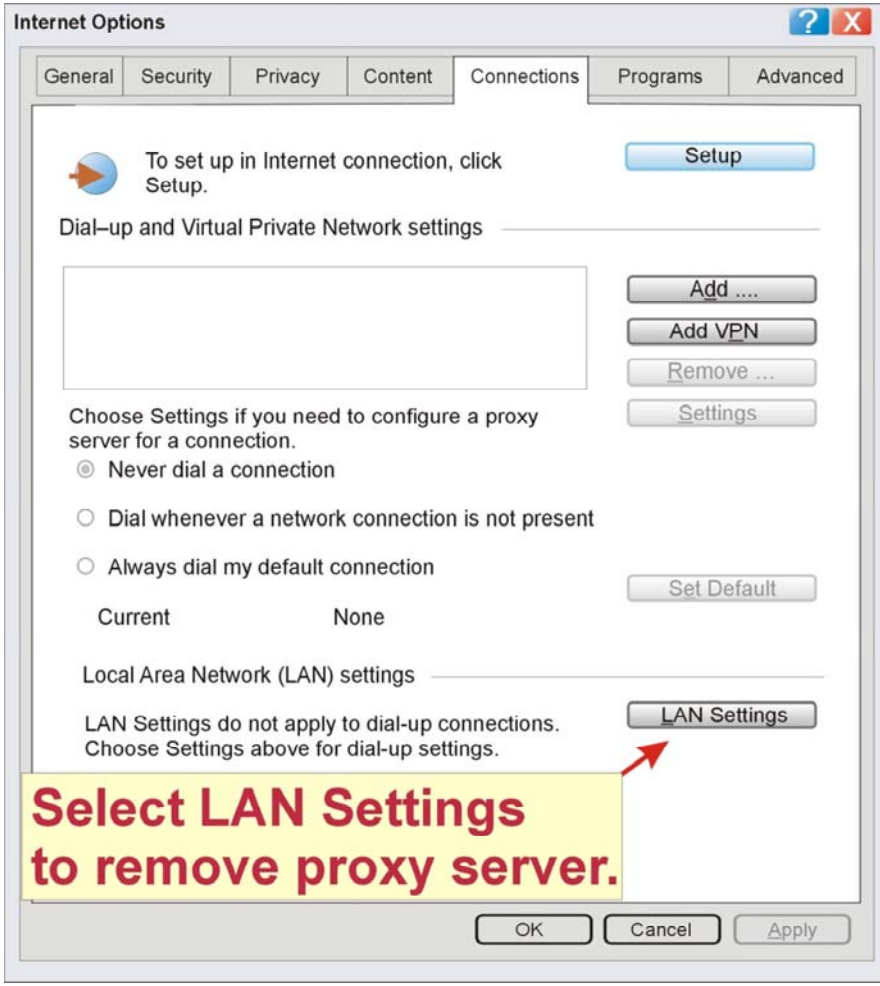


Figure 4 - 2 Internet Options Panel

When the (Local Area Network) **LAN Settings** panel shows that the **Automatically detect settings** or that **Use a proxy server for your LAN** boxes are checked, Internet Explorer is then using a proxy server which

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

blocks it accessing the Internet. Figure 4 – 3 Internet Explorer Proxy Server Enabled shows these settings.

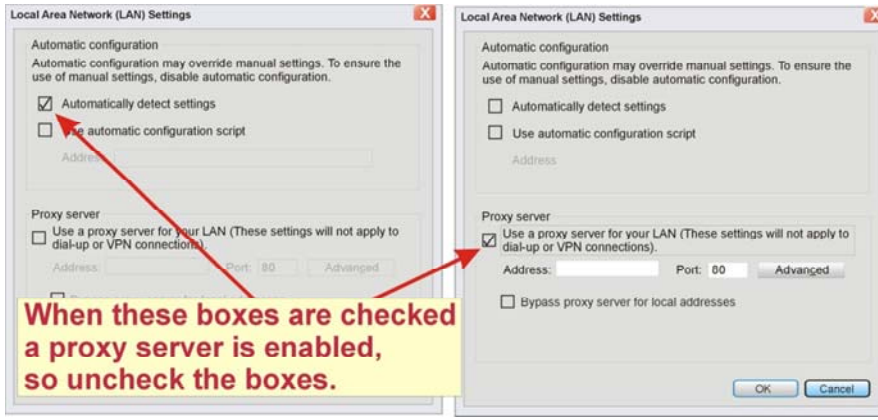


Figure 4 - 3 Internet Explorer Proxy Server Enabled

When the proxy server boxes are unchecked, the proxy server is disabled as shown in Figure 4 – 4 Internet Explorer Proxy Server Disabled.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

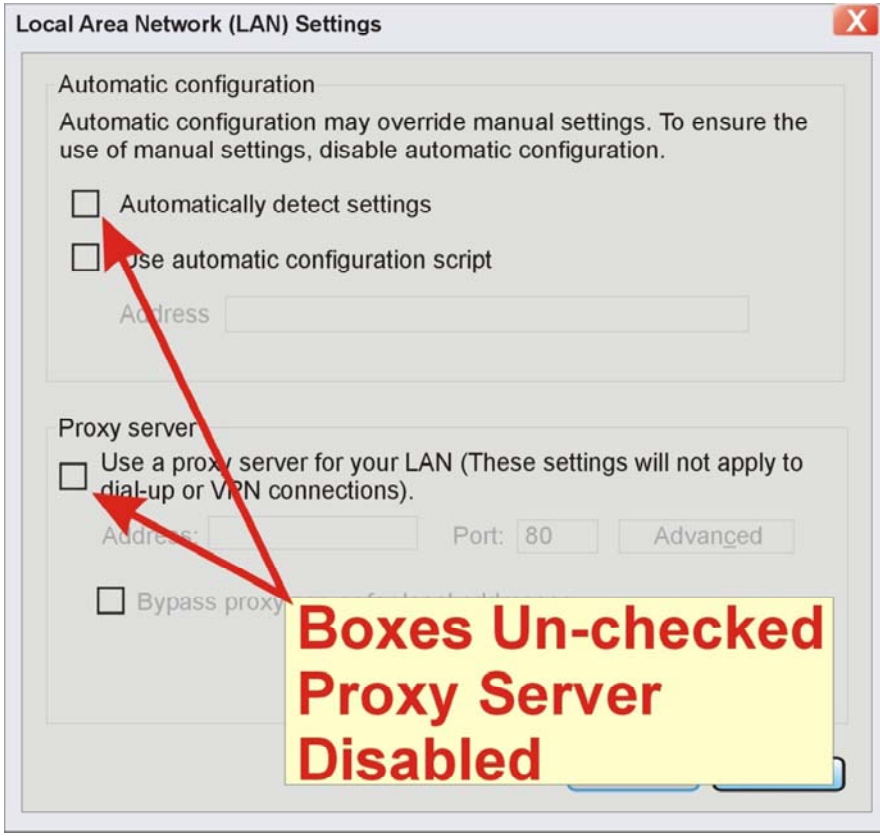


Figure 4 - 4 Internet Explorer Proxy Server Disabled

Firefox is similar configuration settings. To change the proxy server on Firefox first open Firefox menus by clicking on the down arrow in the upper left-hand corner of the Firefox web browser. This displays the Firefox navigation menus as shown in Figure 4 – 5 Firefox Navigation Menus.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

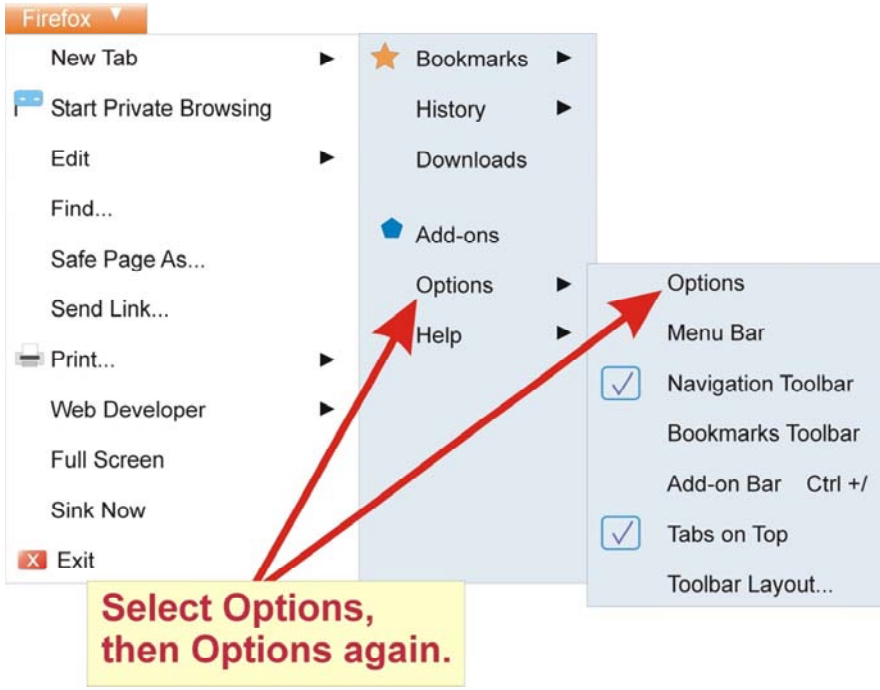


Figure 4 - 5 Firefox Navigation Menus

Using the menus select **Options** and then select **Options** again to get to the Firefox configuration options. This opens the Firefox configuration options panel as shown in Figure 4 – 6 Firefox Configuration Options Panel.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

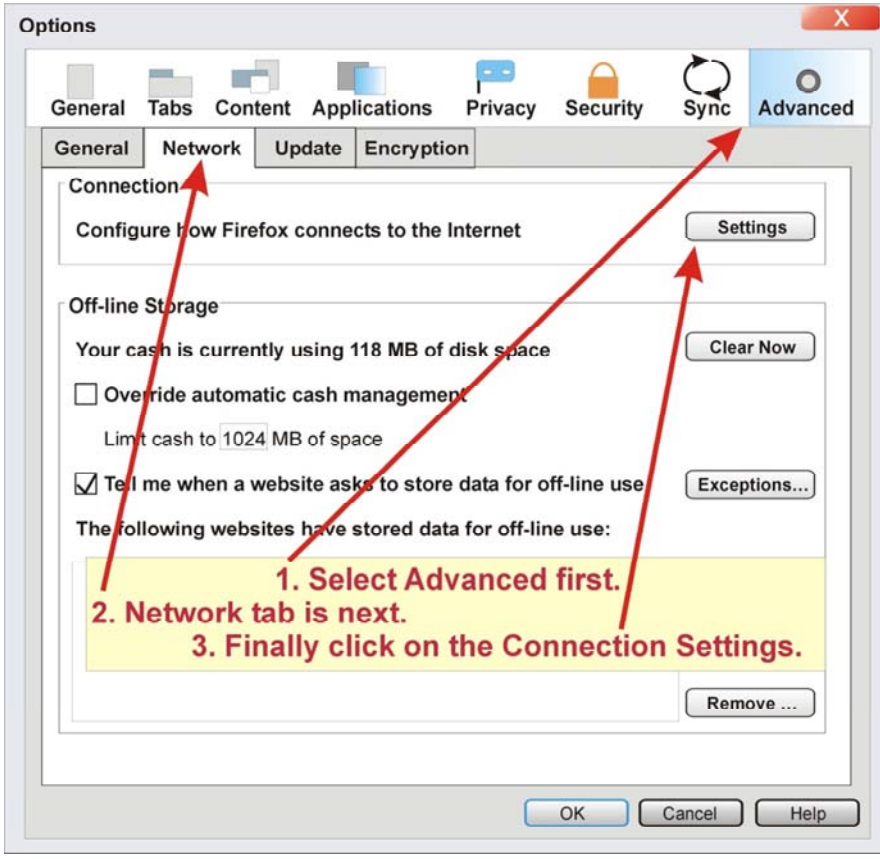


Figure 4 - 6 Firefox Configuration Options Panel

When the Firefox options menu is displayed select the **Advanced** tab. In the **Advanced** menu please select the **Network** tab. The first item in the **Network** tab is the **Connection** option. This option controls how Firefox connects to the Internet. Clicking on the **Settings** button opens up the connection settings panel.

The Firefox Connection Settings panel shown in Figure 4 – 7 Firefox Connections Settings Panel shows on the left the **Use system proxy settings** button selection so that Firefox uses the same proxy server as the Internet Explorer. This setting often enables a proxy server for Firefox. By

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

selecting **No proxy** as shown in the right-hand Options panel in Figure 4 – 7, all proxy servers are disabled in Firefox and Internet Explorer as well.

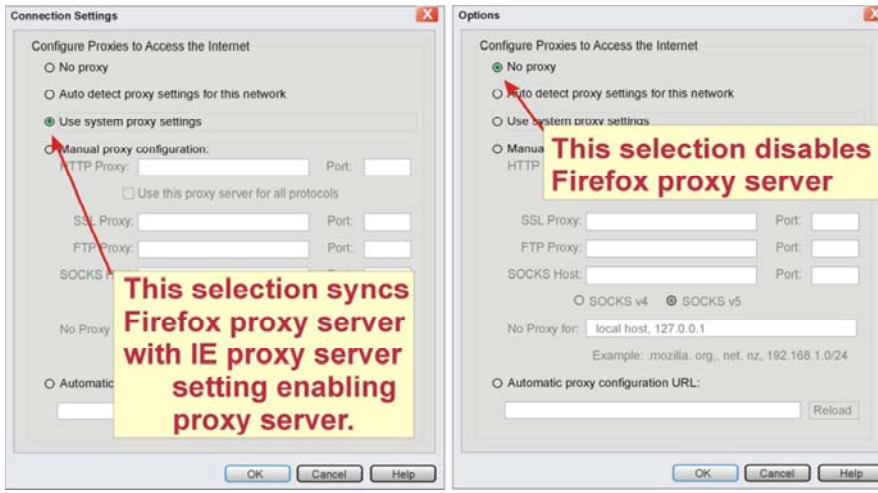


Figure 4 - 7 Firefox Connections Settings Panel

After disabling such proxy servers, both Internet Explorer and Firefox should be able to browse the web and display websites.

Damage Type 2 – EXE Files Do Not Run

Shortly after I started this book, a friend brought in their computer that was infected by a virus. They knew it was infected by a virus because messages popped up on their computer's display saying that it was infected by viruses, identifying several infecting viruses, and offering to remove these viruses. This message was the virus itself. The viruses it identified were false positives. They were identified in order to incentivize the hapless victim to purchase the virus removal package they were selling. Once the package was purchased, a key would then cause these virus identification messages to no longer appear because there are really no viruses to remove.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Additionally, this virus blocked running any EXE programs. The most common program file extensions are EXE and DLL. In the early days of computers there were also COM programs. The differences between these types of programs are that the COM programs ran in the lowest parts of memory (the first 640 KB), while EXE and DLL programs run anywhere in memory. Today's Windows 7® computers typically have 4 GB of memory. Early Windows® computers worked with 1 MB of memory. Finally, EXE programs are often the programs that launch other programs. The DLL programs are called by the EXE programs to do specific functions within an application. For example in Microsoft® Word there is a DLL program that performs the spelling check function. Virus removal programs are EXE programs. When EXE programs cannot run, no virus removal programs can run.

When an EXE program is blocked from running, Windows® displays an error message that asks you to select the program used open this file. This is confusing to everyone because it seems that you have a data file you wish to open, but can find no program to open it. The error messages a lie. It is a rare occasion when you find something that lies more than a politician. Windows® error messages are always lies. This is because the root source of the error is far removed from the program that creates the error message.

Nerd Tip: *The words in an error message can be searched using Google® or Bing® to help find a solution to that error. Such searching often leads you to forums where Internet users present questions and other knowledgeable users attempt to answer them. These answers are often a shot in the dark at resolving the error. The best approach to use in attacking such errors is to step back and ask yourself what is the likely source of the error? Is the error caused by a Registry entry? Is the error due to a missing program file? Is the error caused by a hardware failure? The forum answers can help guide you in determining the area (Registry,*

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

program, or hardware) that is the root source of the error but the rarely resolve the error.

What part of Windows® do you think causes the EXE files not to run? Is it a corrupted Windows® program? Is it a hardware problem? or Is it a Registry problem? Are you clueless? Then let's think of this logically. Viruses generally add programs to Windows®. Some viruses may incorporate themselves to normal Windows® programs. These two actions do not block EXE programs from running. Viruses also alter the Registry. Altering the Registry causes a wide variety of Windows® errors including blocking EXE programs from running.

Nerd Tip: *A possible quick fix to this problem is to locate Malwarebytes® on your computer, click the right mouse button and select from the drop down menu "Run as administrator". Update Malwarebytes® as required and run the "Perform full scan". Then also run Spybot as an administrator. These programs combined are likely to mitigate the problem.*

Nerd Tip: *The best source for resolving Windows® errors are corporate sites like Microsoft® and Symantec®. Because the answers found in forums are from inexperienced users, they are often incorrect. There is certainly some insight to be gained from every answer. However, the answers themselves are not the "needle in the haystack" or the "silver bullet" that fixes a Windows® problem.*

Most often when Windows® becomes corrupted it is not because Windows® programs have been removed or altered. Windows® becomes corrupted when the Registry is changed. Windows® System Restore can return the Registry to an earlier version removing the Registry corruption fixing Windows®. The problem is that there may not be enough restore points to have saved an uncorrupted version of the Registry that fixes the problem.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

In the early Disk Operating System (DOS) computers, two files AUTOEXEC.BAT and CONFIG.SYS controlled DOS. As computers migrated from DOS to Windows® Microsoft® developed more complex control structures. In early versions of Windows® these control structures were WIN.INI and SYSTEM.INI. These two files were the predecessor of the Registry used in Windows 2000®, Windows XP®, Windows Vista®, and Windows 7®.

Nerd Tip: *Anyone copy of their own Windows® Registry. In this manner they can make a backup copy of the Registry independent of the Windows® System Restore function. The Registry is found in the C:\Windows\system32\config folder. Copying this folder to another drive or to a different location on the same drive makes a duplicate copy of the Registry at that instant in time. It is possible to use this copy to restore the Registry back to its state at that exact point in time. This is like making a Polaroid® photograph of the Registry.*

The Registry groups control information for Windows® and Windows® applications programs into hierarchical information structures called hives. In the Registry there are five hives. See Figure 4 – 8 Windows® Registry Hives.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

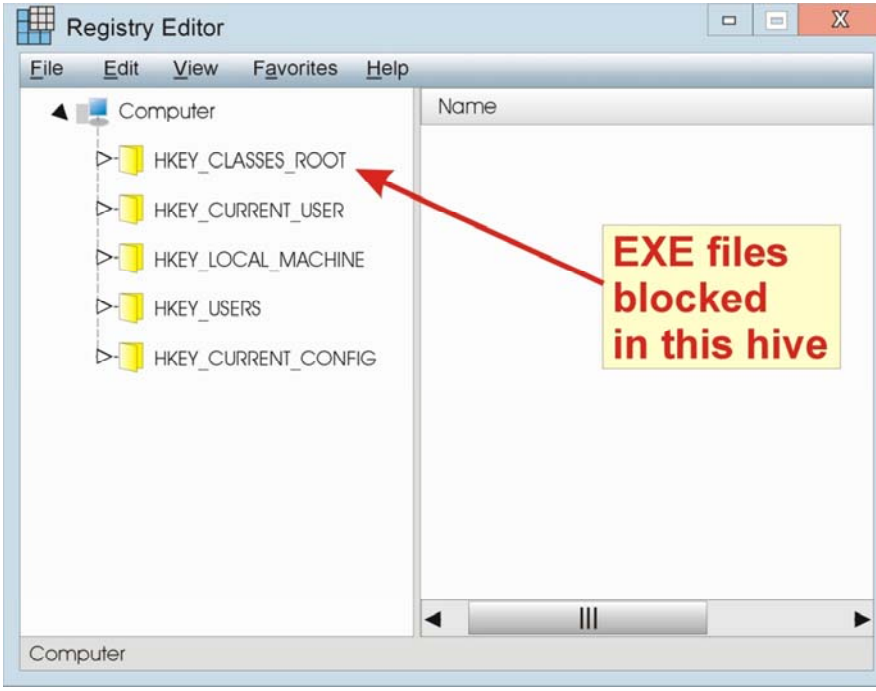


Figure 4 - 8 Windows® Registry Hives

EXE files are blocked from running by changes to two entries in one of the hives. This hive is identified as HKEY_CLASSES_ROOT.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

The two entries are:

1. **.exe** and
2. . **exefile**

entries. The problem is how do you fix those entries and get EXE files to run when you cannot run and EXE file. There is a solution.

This problem is unique to each user account. So it impacts only a single user account at a time. To resolve this problem, use the Control Panel and the User Accounts and Family Safety category to add a new user account to the computer. This new user account must have full administrator privileges. In creating the account is unimportant what name you give it but it is most important to create it with full administrative privileges and no password to make it easy on yourself logging into the account. Once the repair procedure is completed, this account can be deleted in its entirety.

After the account is created, log out of the current account. This does not mean to shut down and restart the computer but merely to log out of the existing account so that you can log into the newly created account.

After you have logged into the new account in Windows® has settled down, click on the start button and in Windows XP® enter Regedit in the Run entry area or in Windows Vista®/Windows 7® enter Regedit in the Search programs and files entry area. Please strike the Enter key next to run the Registry editor.

When the Registry editor starts, it picks up from where it was last used. This can be confusing because it may be deep down into the Registry hives and not close to where it is helpful to us. Fortunately, the Registry is easily navigated using the keyboard of your computer.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

When the Registry editor is opened it displays two panels. Use your mouse to click on the left panel. It does not matter where you point as long as the Registry editor is active in the left panel. Now use the left arrow key to navigate to the top of the Registry hives. Keep tapping the left arrow key until you see only one entry in the Registry editor. This entry should say Computer. After you reach the top Registry entry, tap the right arrow key once. This should cause them Registry editor to display the five hives. To fix the EXE file problem we change Registry entries in the first hive, HKEY__CLASSES_ROOT. See Figure 4 – 9 Registry HK_ CLASSES_ROOT.

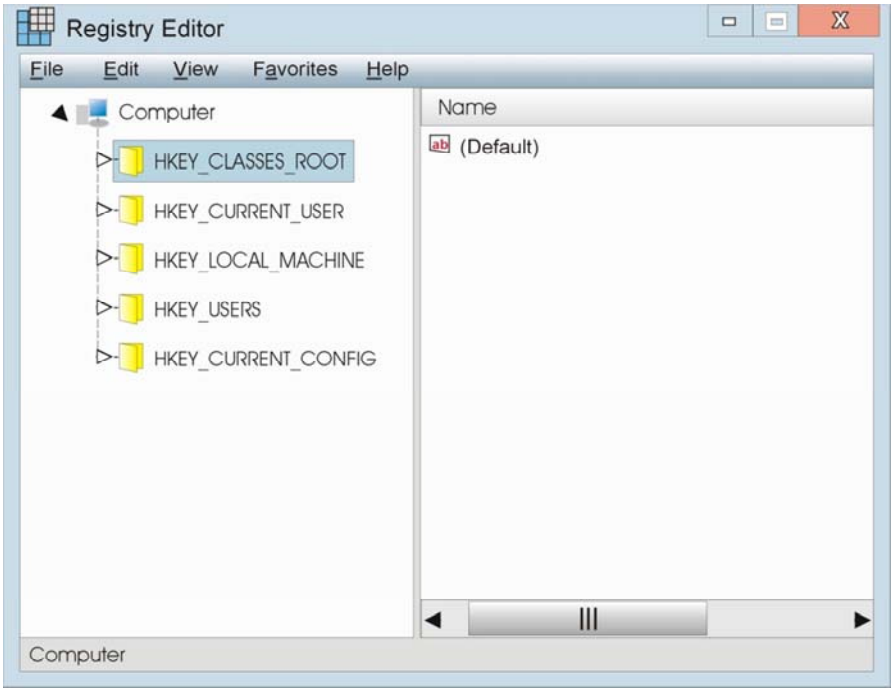


Figure 4 - 9 Registry HK_ CLASSES_ROOT

Next tap the down arrow key once to select the first hive. Tap the right arrow key to expand the hive. Many hive entries appear. All the hive

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

entries are in alphabetical order with punctuation symbols and numbers coming first.

The first time entry under

HKEY_CLASSES_ROOT is: *

The next entry is: .123

When you tap the page down key about four or five times, you should be able to see the "**.exe**" Registry key in the left panel as shown in Figure 4 – 10 HK_ CLASSES_ROOT dotexe Key. Watch the left panel keys closely to make sure that you do not pass the "**.exe**" Registry key. If you do pass it, use the page up key to move back up the Registry and locate the key. Now point the key with your mouse and click the left mouse button to highlight it. Once this highlighted click the right mouse button and select export from the drop-down menu. The Export Registry File window appears. Click on the desktop icon on the left side to save this Registry key to your desktop. Where it says "File name:" enter an appropriate filename.

My preference is the name the file so that the key is easily identified. Something like HKCRdotexe is good. When the file is saved, Windows® automatically adds the extension .REG.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

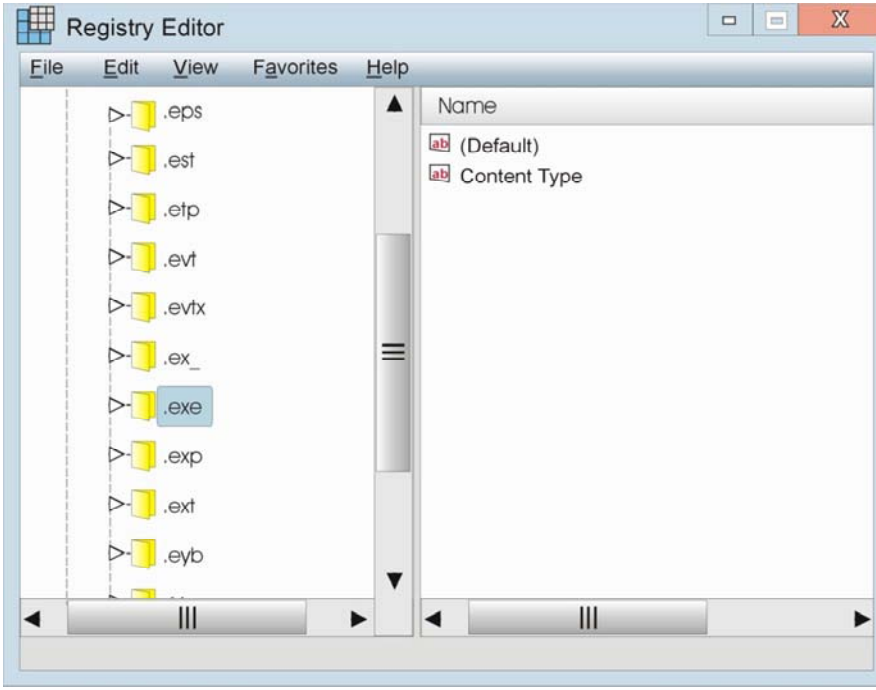


Figure 4 - 10 HK_ CLASSES_ROOT dotexe Key

To quickly navigate to the "**exefile**" Registry key, please type the "F" key. This should jump you to the entries beginning with "F" in the HKEY_ CLASSES_ROOT hive. The entry you should land on is "FaultrepDataCollectionInProc". About eight injuries above that key should be the "**exefile**" Registry key. This is shown in Figure 4 – 11 HK_ CLASSES_ROOT exefile Key. Please repeat the export process described above to export this key to your desktop. A good name to use for the file is HKCRexefile.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

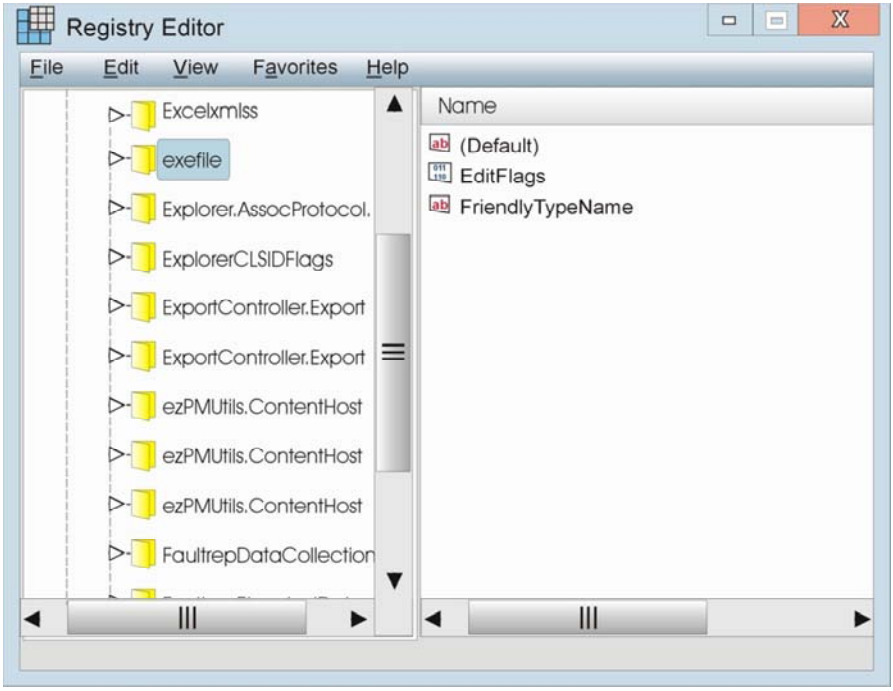


Figure 4 - 11 HK_ CLASSES_ROOT exefile Key

These two Registry files are the tools needed to permit EXE files to run under your user account. Sometimes only one of these keys is damaged and needs to be replaced. But if both keys are damaged, like good Boy Scouts and Girl Scouts we are prepared.

The Registry editor can now be closed by clicking on the X in the upper right-hand corner. After the Registry editor is close, locate the two files we just saved on your desktop. Please remember that this is the desktop of the new user that you just recently created. It is not the desktop of your original user account. This means that we need to copy these two files to a location on our disk drive that can be accessed by all user accounts. The most universal place I can think of is in the root directory of drive C:. Please be sure to copy to that location and not just move them. To do that click the right mouse button, select copy from the drop-down

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

menu and then paste them in the root folder of drive C:. After that is complete, log out of this new account. Please remember to not shut down and restart the computer but just to log out of the account.

Nerd Tip: *The Registry is easily navigated using the keyboard keys. When the left Registry editor panel is active the left arrow key closes up the hive entries and the right arrow key opens them up the down arrow key will move into the entries below the active Registry key. These entries are all in alphabetical order with punctuation symbols and numbers coming first in the order and the alphabetical characters coming second. Knowing this it is easy to page up page down watching the alphabetical order to locate a specific key in a Registry hive. It is also possible to jump close to that key by tapping the first letter in the key name. Sometimes it's faster to type the next letter in alphabetical sequence and work backwards towards the key than to move downward in the list of keys. Tapping a letter several times causes the Registry editor to jump down one entry at time for each tap of the key.*

Now you may log into your old user account. Use the Windows® Explorer to navigate to the root folder of drive C:. Locate the exported Registry files that were just copied to that location. You may click the right mouse button and select "open" from the drop-down menu or just double-click on the Registry file. This causes the file information to be entered into the Registry for your old account. Do this for both Registry files. Now EXE programs should run properly. The next step is to repeat running Malwarebytes® and Spybot Search & Destroy. These programs should clean up the remaining bad Registry entries that blocked the EXE files from running. After both these virus removal programs finished running, the EXE files damage to your computer should be repaired.

Damage Type 3 – Your Data Has Disappeared

The case of the disappearing data is a crime of "magic". It is a crime of "magic" because the data has not been erased, but rather merely hidden

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

from you. Because the file and folder attributes are set to System and Hidden Windows® you can no longer see them and application programs can behave strangely and irrationally.

Windows® data is stored for each user account and each default account in either the Documents and Settings folder (Windows XP®) or the User (Windows Vista® or Windows 7®) folder. Figure 4 - 12 Windows XP® User Account Folders Normal Settings shows the normal folders including the hidden folders under the user account Pete. The folders that are not hidden are the Desktop, My Documents, and Start Menu folders. These folders have the brighter icons in Figure 4 - 12.

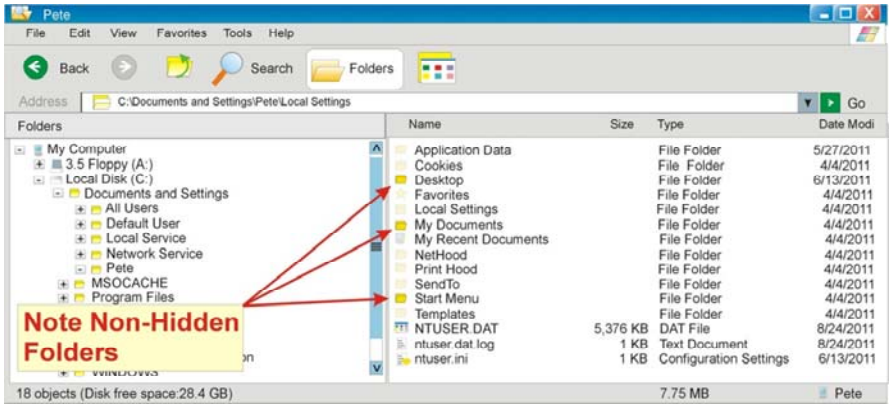


Figure 4 - 12 Windows XP® User Account Folders Normal Settings

When the hidden folders such as the Application Data folder are opened, the folders below that folder are not necessarily hidden folders. Windows® programs rely on information in the hidden Application Data folder. They also count on the data not being hidden data. When the contents of the Application Data folder are also hidden, Windows® programs often behave strangely.

When a virus marks all folders as System, Read-only, and Hidden; the user's data appears to vanish and Windows® programs behave erratically.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Figure 4 - 13 Windows XP® User Account Folder Attributes Set As Hidden shows all folders as greyed out and marked as Hidden.

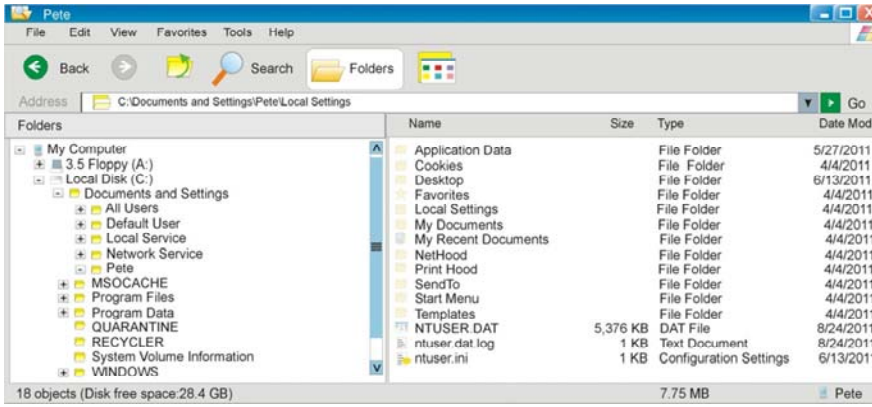


Figure 4 - 13 Windows XP® User Account Folder Attributes Set As Hidden

Checking the folder status with the Windows® Explorer set at default settings would show nothing under the user account as illustrated in Figure 4 - 14 Windows XP® User Account Folder Hidden Attributes Seen With Default Explorer Settings.

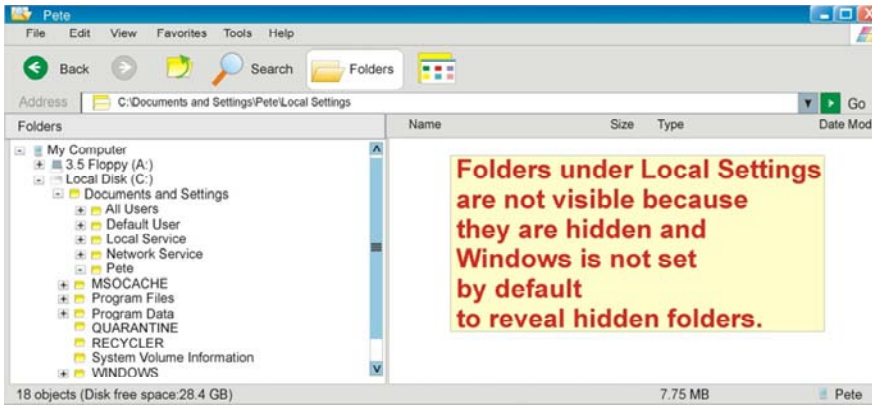


Figure 4 - 14 Windows XP® Folder Hidden Attributes Seen With Default Explorer Settings

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

In Chapter 3 we set up Windows® Explorer to view hidden folders. The procedure is described again here. Changing final settings for Windows® Explorer to permit viewing of System and Hidden files is the same, but the setting location has changed between Windows XP® and Windows 7®. In Windows XP® the **Folder Options** settings are found under Tools and **Folder Options…** as shown in Figure 4 - 15 Windows XP® Folder Options.

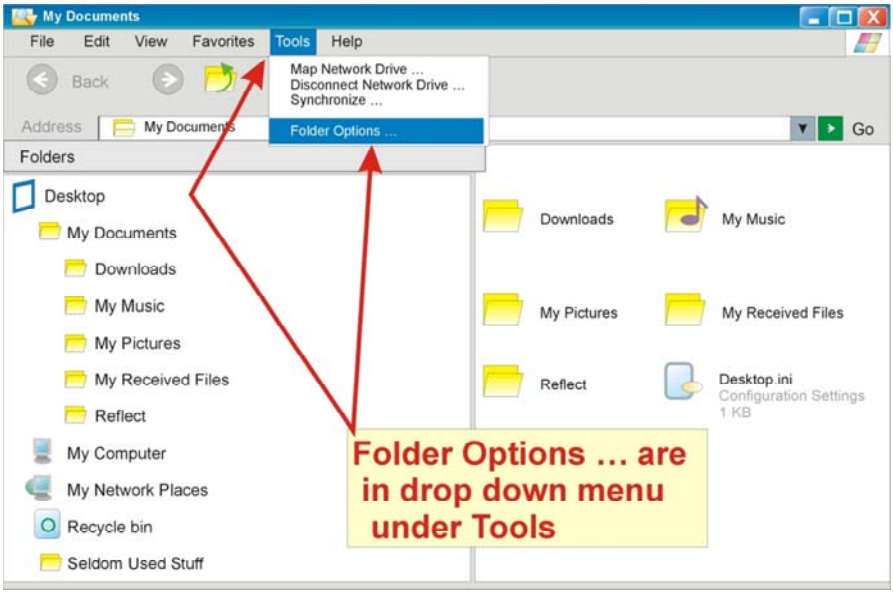


Figure 4 - 15 Windows XP® Folder Options

In Windows 7® (and Vista®) the Folder and Search Options menu selection leads to the **Folder Options** menus. The Folder and Search Options are found under the **Organize** menu selection. See Figure 4 – 16 Windows 7® Folder and Search Options. This can be hidden from view depending upon the setup of Windows® Explorer. Windows® menus have become "context sensitive". This means that often the full menu selections available to the user are not visible to the user. Sometimes **Organize** is hidden from view. So you may need to find it.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

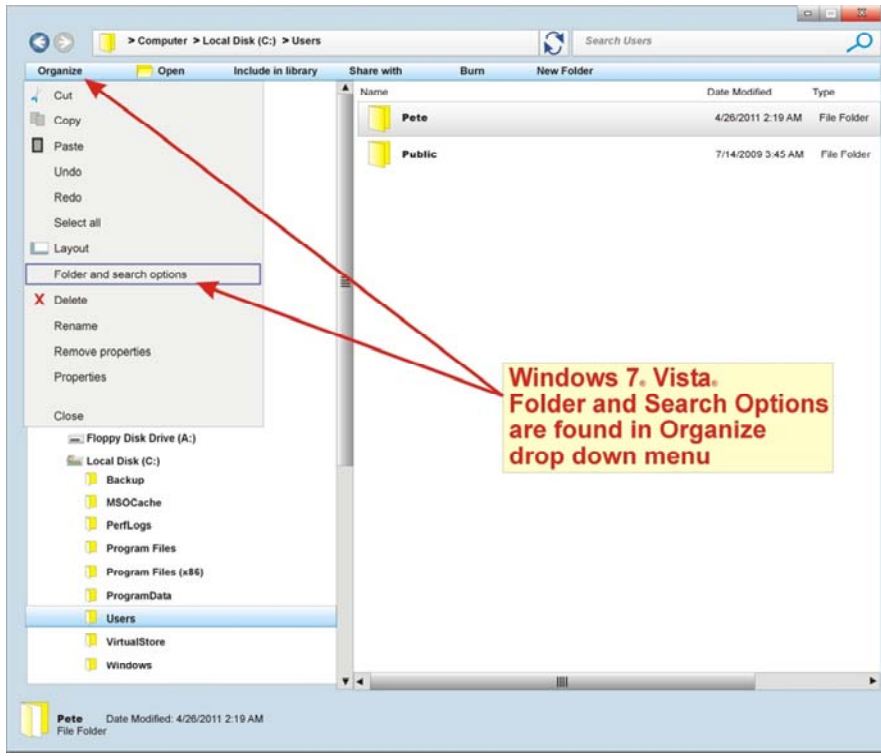


Figure 4 - 16 Windows 7® Folder and Search Options

Clicking on the **Folder Options** or the **Folder and Search options** leads to the Folder Options panels. These panels configure Windows® Explorer to show the Hidden and System files as shown in Figure 4 – 17 Windows® Folder Options.

Nerd Tip: *An easy way to get the Windows® Explorer file options menu is to use the keyboard shortcuts. When the Windows® Explorer is the active window, holding down the ALT Key and tapping the F key brings up the File menu and the Folder and search options menu selection in Windows® Explorer.*

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

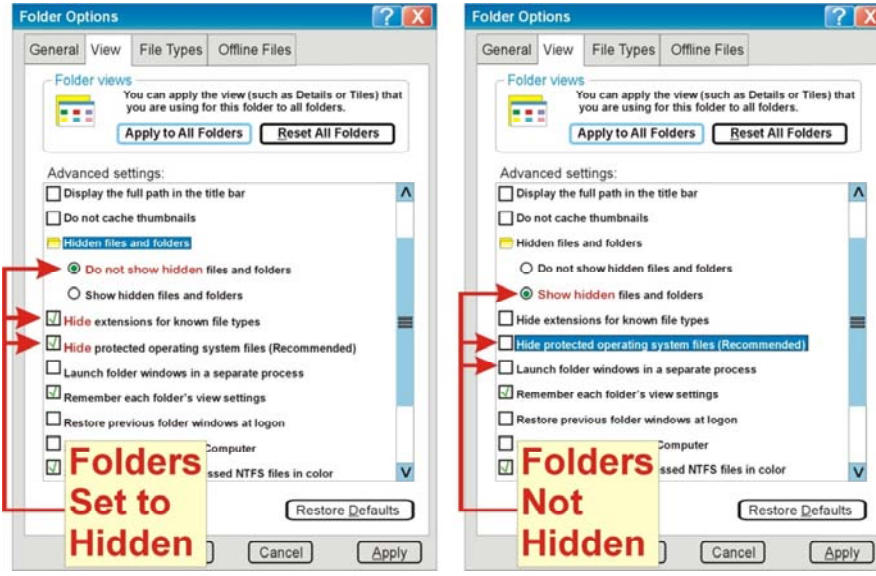


Figure 4 - 17 Windows® Folder Options

Checking the Show hidden files and folders and unchecking the Hide Extensions and the Hide protected operating system files permit Windows® Explorer to reveal the data that seemingly vanished.

Resetting the files to make them usable again is another matter. This requires changing the file attributes from Hidden, System, and Read-only. The good thing is that by making all files the same not Hidden, not System and not Read-only they become usable again. There is no need to check each file or folder to determine how that file or folder should be set. Just set them all to not Hidden, not System and not Read-only and open the security level so that the Windows® Group Everyone has full control of the files. If needed, have the group Administrators take ownership of all the files in the users account folder.

There are two way to change the attributes of Windows® files and folders. First you can use the command console and the **ATTRIB**ute command. Second you can use the Windows® Explorer to change the Security and the

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

file properties. The quickest and easiest if it works is to use the command console and the **ATTRIB**(ute) command.

To use the Command Console click on the START button to reveal the opening Windows® start menu. Select All Programs and Accessories to find the Command Prompt shortcut as shown in Figure 4 – 18 Windows® Command Console Location.

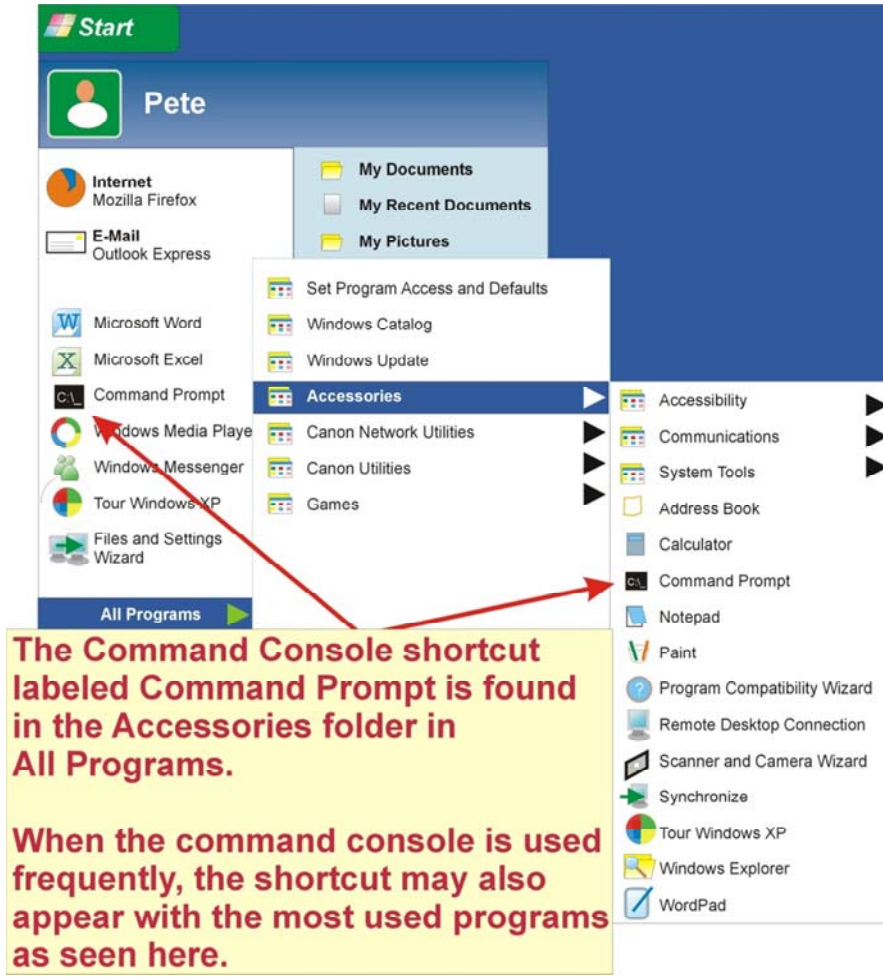


Figure 4 - 18 Windows® Command Console Location

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Once the command console is started you have a black window with the command prompt. Sometimes people worry about the text displayed on the screen. That text just describes the folder that the command console is currently working upon. In Figure 4 – 19 Command Console ATTRIB Command the command console is pointing at the folder C:\Users\Pete.

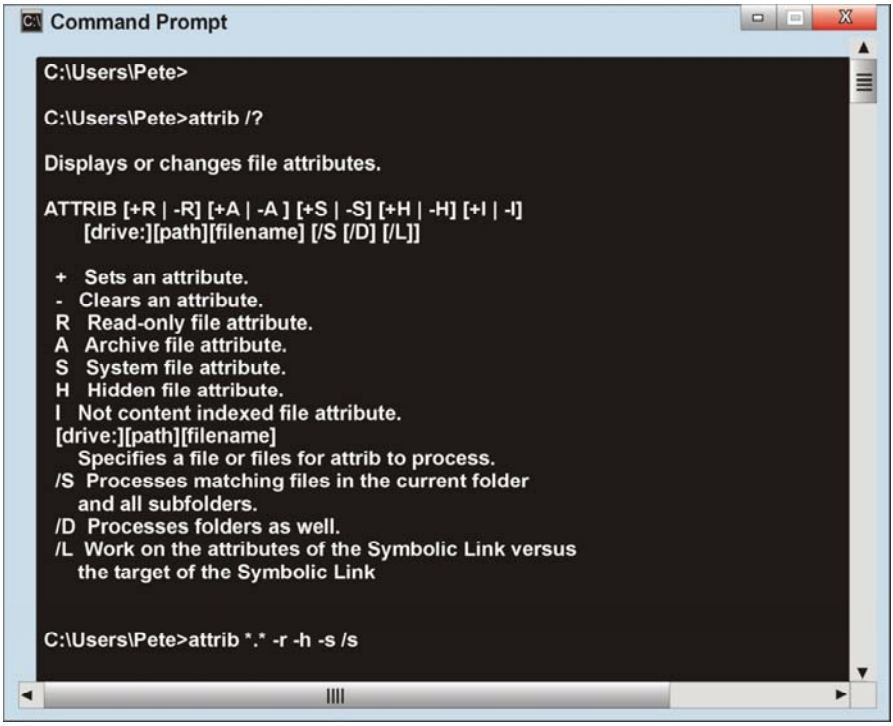


Figure 4 - 19 Command Console ATTRIB Command

When the command **ATTRIB /?** Is entered, Windows® responds with the help message that shows the command options and what they do.

To reset the user account the ATTRIB command is used. Log on to the user account to be reset. Open the command console and enter the command: **attrib *.* –r –h –s /s**

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

This command resets the r-Read-only, h-Hidden, and s-System for all the files, folders, and sub-folders in C:\Users\Pete. This should restore the missing data.

It is possible that the virus can block resetting the attributes by changing the security permissions on files and folders. In this case it is necessary to use the second approach resetting the files and folders with Windows® Explorer. This approach permits resetting file and folder security permissions as well as the file and folder attributes.

To reset the files and folders with Windows® Explorer, please point to the user account folder. In our example the folder is C:\Users\Pete. This is a Windows 7® computer account folder. After the folder is selected – highlighted – click the right mouse button and then click on properties at the bottom of the pop-up menu as shown in Figure 4 – 20 Folder Properties. The folder properties should pop-up and have the General tab selected. In the General tab the folder attributes Read-only and Hidden attribute settings are shown. See Figure 4 – 21 Folder General Properties. Before these settings can be changed we need to first reset the folder's security.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

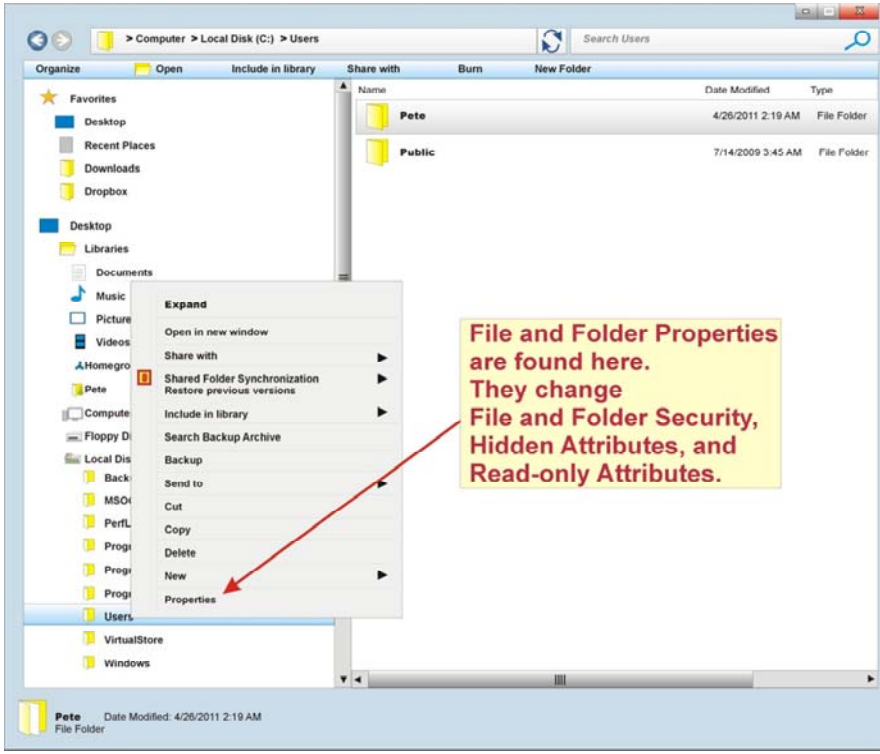


Figure 4 - 20 Folder Properties

Folder security generally flows downhill like water. The security set at the top folder becomes the security at the sub-folders under that folder. Sometimes security flowing down into the lower folders causes indigestion and comes back up.

Folders with security set specifically at a lower level folder do not permit the security flowing down from the upper folder to change that security setting. This blocks resetting file permissions at the lower folder. So the permissions must be specifically set at that lower folder or on the blocking file in the lower folder to complete resetting all the permissions.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

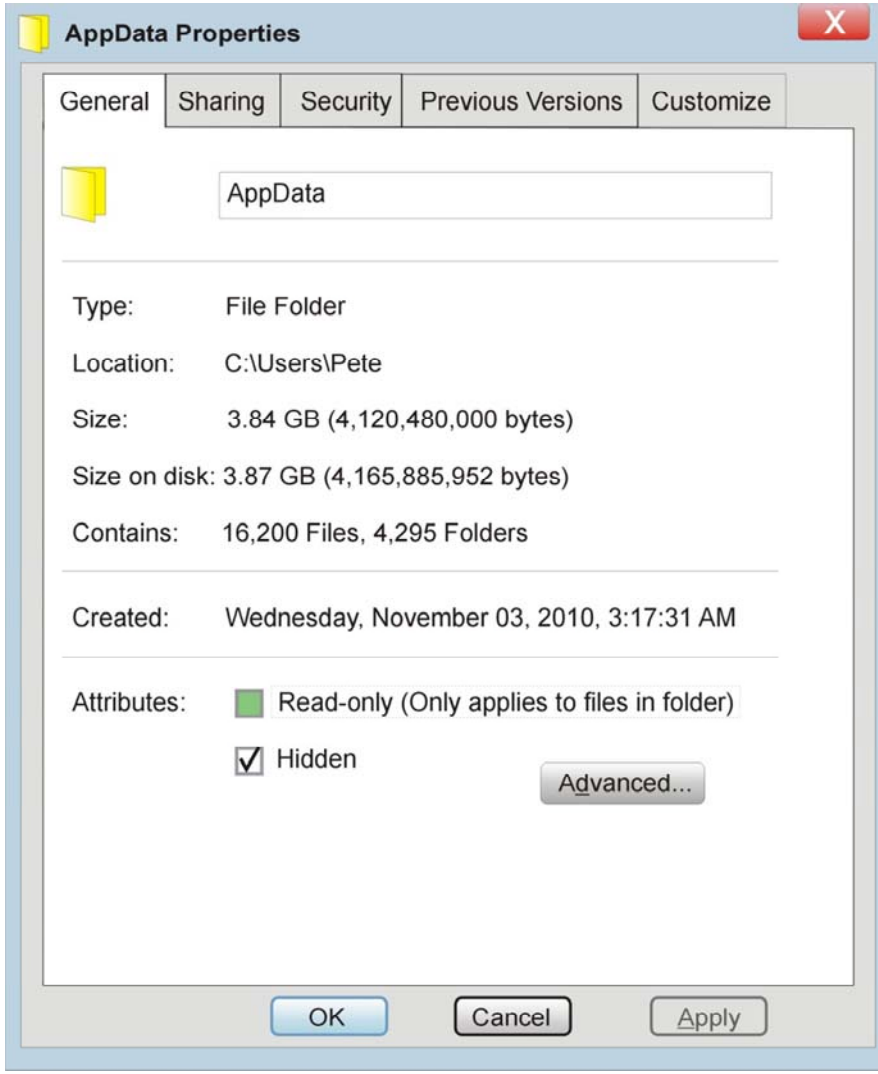


Figure 4 - 21 Folder General Properties

When the security tab is opened, the Group or user names are displayed in the first panel, and the permissions for the highlighted Group or User are displayed in the bottom panel.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Between both panels is the **Edit…** button. Clicking on the **Edit** button permits a new Group or User to be added. To loosen up the security on the folder and files, we want to add the Group Everyone. To do that click on **Add**, then type Everyone in the open typing area in the Select Users or Groups panel, and click **OK**. This is shown in Figure 4 – 22 Folder Security Settings.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Once the group Everyone is added, please set their security permissions to Full Control. Click on apply or OK to set the security permissions. If the change in permissions is blocked, the ownership of the folders may need to be changed first.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

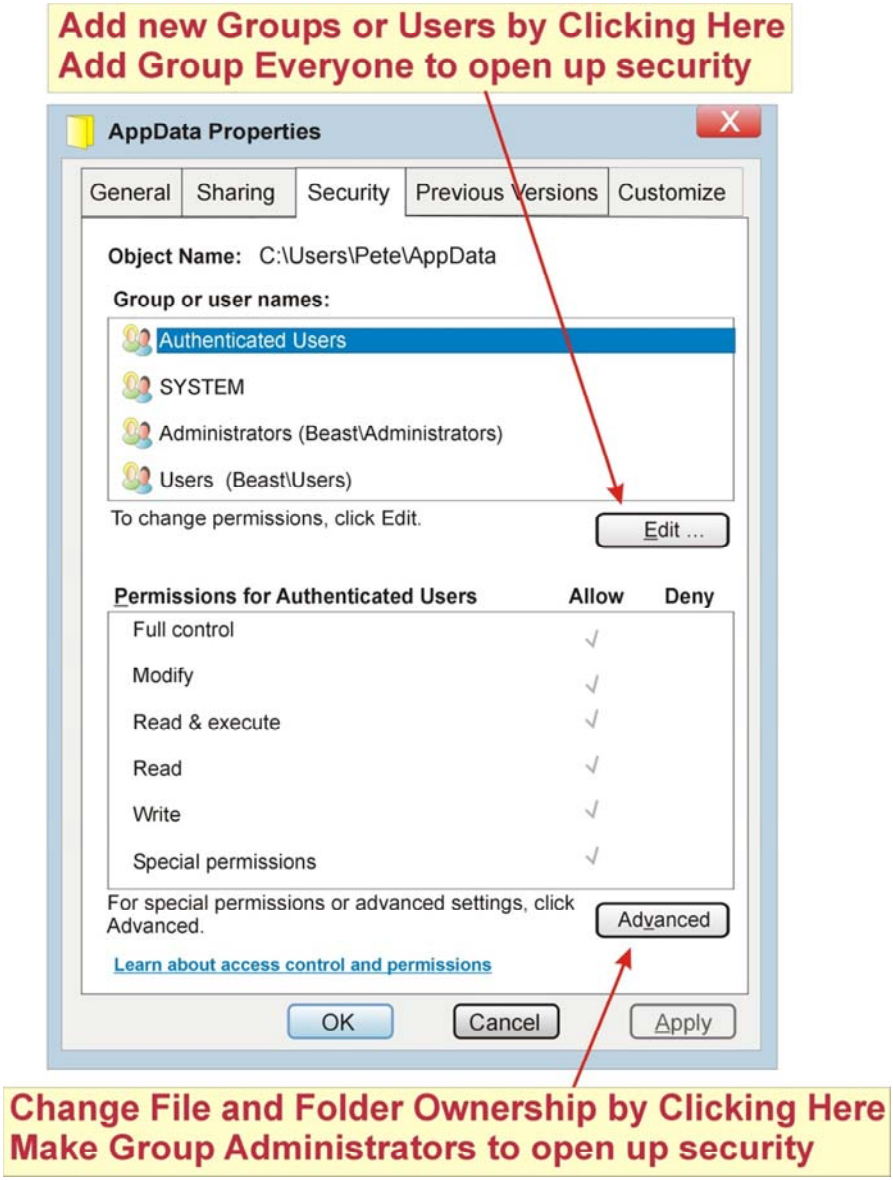


Figure 4 - 22 Folder Security Settings

To change the ownership of the Folders and Files click on the **Advanced** button at the Security tab in the initial properties panel. The **Advanced**

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Security Settings panel now opens. See Figure 4 – 23 Windows 7® Advanced Security Settings Panel.

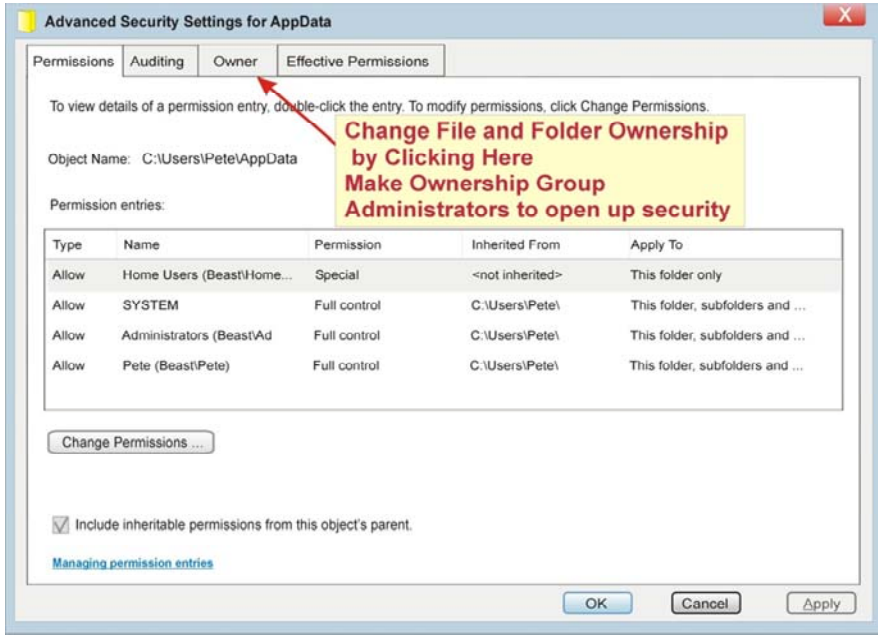


Figure 4 - 23 Windows 7® Advanced Security Settings Panel

The second tab from the left is labeled **Owner**. This is shown in Figure 4 – 23. Clicking on it reveals that the current owner is the user of the account as revealed in Figure 4 – 24 Windows 7® Advanced Security Settings Owner Tab.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

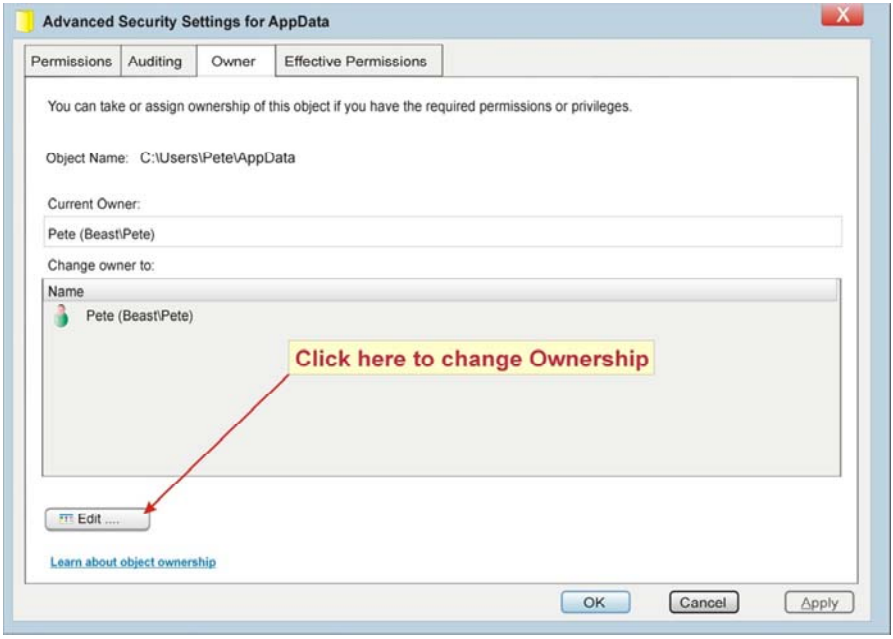


Figure 4 - 24 Windows 7® Advanced Security Settings Owner Tab

At the lower left of the owner tab is an **Edit…** button. Clicking on it opens the **Advanced Security Settings Owner** panel showing that the account user and the group **Administrators** can be designated as owners of these files and folders. See Figure 4 – 25 Windows 7® Advanced Security Settings Edit Owner.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

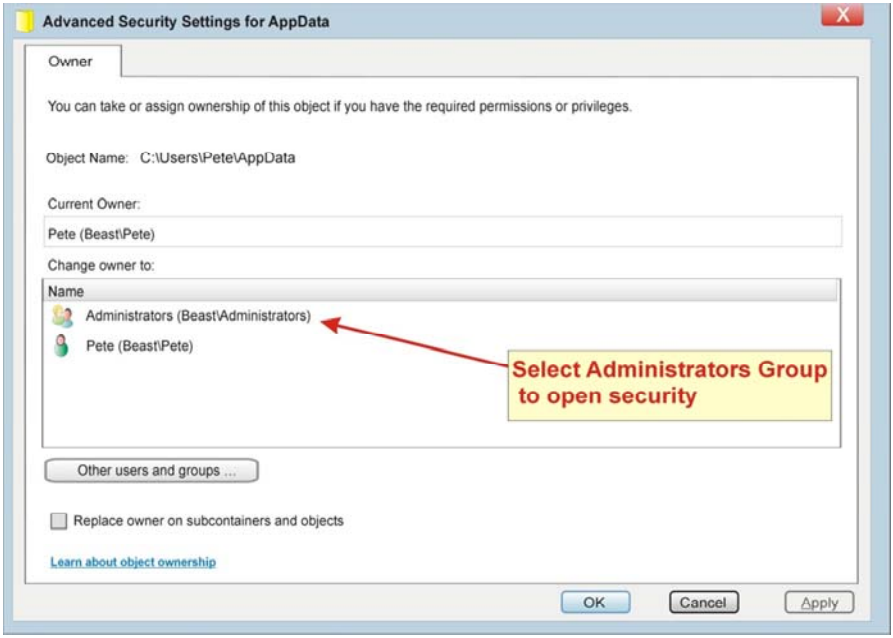


Figure 4 - 25 Windows 7® Advanced Security Settings Edit Owner

Select the **Administrators** group and click **OK**. This changes the owner and some security permissions on the folders in the user account. This is shown in Figure 4 – 25.

You may need to click on OK once or twice for Windows® to complete this change. A message is often displayed stating that changes are not displayed until you exit and re-enter.

After exiting and returning to the folder security properties tab, you can now add the group **Everyone** to the security settings and give them Full Control. This is illustrated in Figure 4 – 26 Setting Folder Security Permissions to Full Control.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

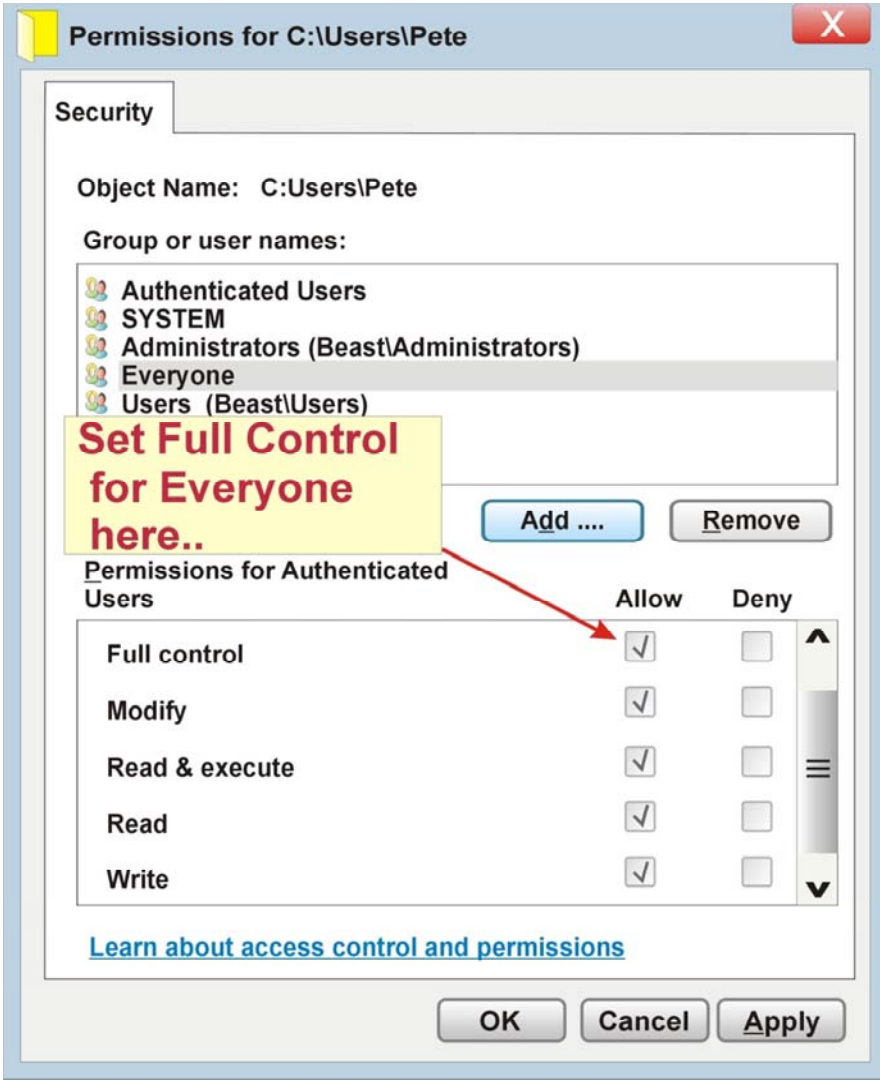


Figure 4 - 26 Setting Folder Security Permissions to Full Control

After Windows® completes resetting the folder permissions, the file attributes can be set to Read-write and not-Hidden at the General tab. Clearing the Read-only and Hidden attribute boxes there and approving

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

the changes, removes those attributes and makes the files once again visible. Figure 4 – 27 Setting File and Folder Attributes illustrates this.

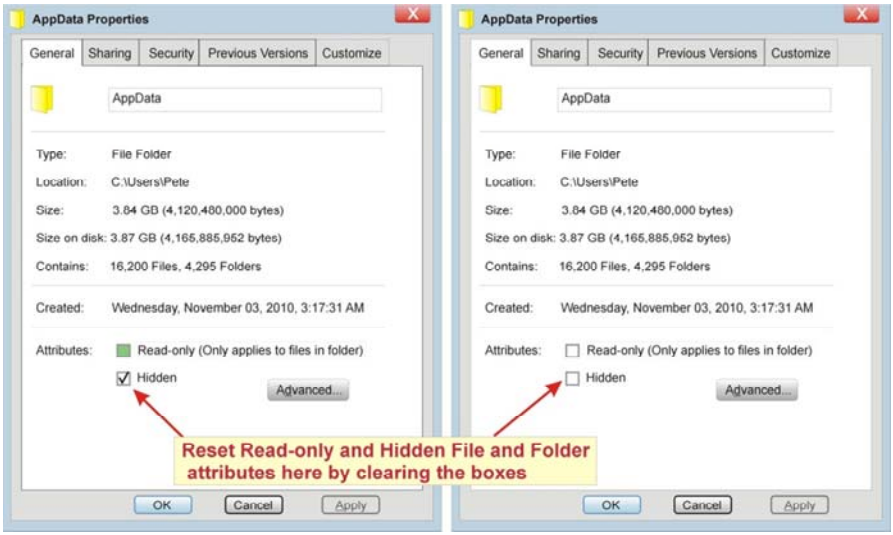


Figure 4 - 27 Setting File and Folder Attributes

These Windows® Explorer menu changes are similar for Windows XP® and Windows 7® (also Vista®). If these fixes still do not solve the missing file problem, the next procedure should. In this case the user account is rebuilt.

Damage Type 4 – Your User Account Is Damaged

More often than not viruses damage the user account so that nothing you seem to do can make the computer behave as it should. The solution to this problem is to completely rebuild the user account. Because each user account operates as though the Windows® computer is its exclusive domain, viruses can clobber one account and leave the other accounts relatively unscathed. After the virus files are removed, rebuilding the user account often solves a myriad of problems.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Rebuilding a user account in Windows XP® is straight forward. Two accounts are typically needed. The Safe Mode Administrator account and the normal user account that is being rebuilt can be used. The Safe Mode default Windows XP® Administrator account is entered by booting into Safe Mode. After logging into the computer as Administrator in Safe Mode, use the Windows® Explorer to rename the user account folder in the Documents and Settings Folder. For example, when rebuilding my account Pete, the user account folder would be named P.

Once the folder is renamed, log out of the Administrative account but do not leave Safe Mode. Immediately log into the user account – in our case here we would log in as Pete. At this point Windows XP® builds a new user account and a new user account folder Pete under Documents and Settings.

To complete the account rebuilding process, log out of the new rebuilt user account but do not exit Safe Mode, and log into the Administrator account again. Now copy the data folders (e.g. My Documents, Application Data, Favorites, the desktop, and any other data folders to the new user account folder. Do not blindly copy everything or the new account can become corrupted. However, copying all the data files, the Desktop, and the Favorites folder saves most everything. See Figure 4 – 28 Windows XP® User Account Folders. If you are using Outlook, then you need to copy the Application Data Folder and the Local Settings Application Data Folders as well. You may need to locate the Outlook PST files, and copy them to the desktop so they can easily be imported into Outlook once Outlook is set up again to transfer all the emails into the new Outlook. Similarly Outlook Express uses DBX files that need to be copied into the correct folder for the email messages to be transferred into Outlook Express.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

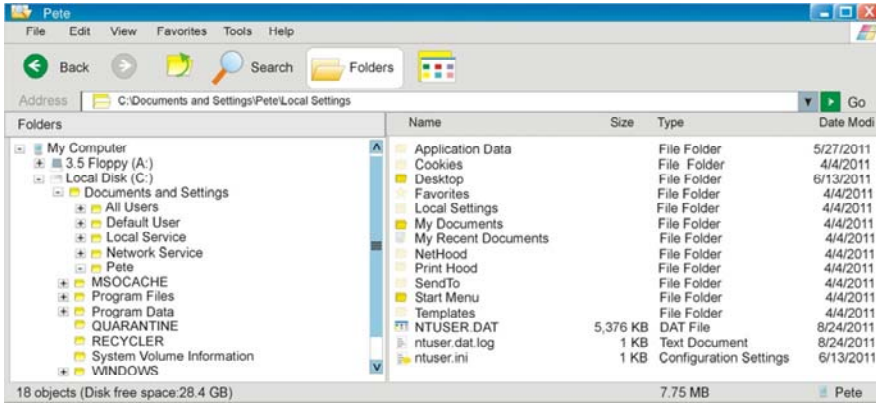


Figure 4 - 28 Windows XP® User Account Folders

Please carefully note that I am using the word COPY here. If you drag and drop folders on the same drive that moves the folders and does not copy them. By copying the folders and data you retain the old data so that you may search it for things that appear missing as you continue to use the recovered user account.

Because Windows 7® (and Vista®) employs added security, recovering the user account is not as simple and direct as it is for Windows XP®. First there is no default Administrative account to use in Safe Mode with Windows 7®. Renaming a user account folder also causes Windows 7® to create a temporary user account folder, but not to rebuild the account. So this is more like a game of checkers where you need to jump around a bit to complete the job.

With Windows 7® the first step is to copy the user account folder to another location. You can make a folder C:\backup and copy the contents of the user account folder there. Next use the Control Panel to create a new account like nerd that has administrative privileges. Please logout of the old user account and log into the newly created account. Use the Control Panel to delete the old user account. You can delete the user files if you have copied them to the backup folder. This may also work if you

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

keep the files, but the old user folder should be renamed so that none of the bad data is retained.

Now recreate the old user account. The old user name can be used if you wish. Then log out and log into the newly created user account. At this point it is a matter of restoring the data to the new account. This is somewhat more complicated because the Windows 7® account folders have a different structure than those for Windows XP®. The files are still there, but the chairs on the deck have been rearranged so you may need to search for specific files to find them. In particular the folder AppData contains the PST and other important data files. These files need to be found using the search function and then imported into Outlook to transfer the emails to the new account.

Nerd Tip: *Outlook email can easily become corrupt and email can be lost because the email messages are in files stored on the computer. Moving to Gmail or Yahoo mail is better because now all the email messages are stored in the "Cloud" and can be accessed from any computer connected to the Internet. There are Calendar and Contact functions equivalent to those in Outlook. More importantly your email messages are safe in the "Cloud" and they can be downloaded and stored on a local disk drive if needed. The only risk is if your email account is hacked so use a strong password and do not let just anyone know what the password is.*

Summary

This chapter has presented and illustrated how to recover from the common damage inflicted on your computer and Windows® by viruses. These problems are caused by a corrupted Windows® Registry and corrupted control files. Restoring the Registry and rebuilding user accounts typically fixes these problems.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

The important thing to remember is not the details here, but rather the problems are in the Registry or in corrupted user accounts. Anything that restores the Registry or corrects the specific Registry damage inflicted by viruses or rebuilds the user accounts fixes these problems and returns your computer to satisfactory operation. In the next chapter we examine the "extreme prejudice" repair, rebuilding Windows.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Please Use This Page for Notes

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

CHAPTER 5
Rebuilding Windows®

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Reinstallation Thoughts

A new potential customer called one day with a problem with their HP computer. It would not boot. So they dropped it by and I began to check it out by running CHKDSK /F. Immediately, the disk drive revealed that it was corrupted. CHKDSK was permitted to run in an attempt to repair the corruption and restore the computer to normal operation. After some time hard disk physical error messages began to appear. The CHKDSK process slowed to the pace of a very slow crawling snail. So I called the computer owner and explained what was happening. I suggested that if the computer was still under warranty she call HP to see if they would ship a replacement drive. She was quite upset and during the discussion she revealed that when the problem first arose that she had tried to correct the problem by running DEFRAG.

DEFRAG is a program that rearranges the deck chairs on a ship so that they are in nice neat arrangements making is easier for passengers to find an open chair next to someone to whom they would like to talk. The problem in this case is that the ship deck was full of holes so rearranging the chairs only exacerbated the problem. That is why I was summoned.

If you suspect any computer problem, never run DEFRAG.

The potential customer called HP and the person they finally got on the line said to stop what I was doing immediately. The HP person was going to solve the potential customer's problem for her by reinstalling Windows XP® on the computer. That is like repainting a ship deck that has big holes in it. There is no amount of paint on this planet that can fill the holes in the deck of a ship thus repairing the deck. Reinstalling Windows® was just not going to work. However, for whatever reason the potential client believed the HP expert and requested that I return the computer. The computer was returned and she was charged nothing.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

When calling for support from a vendor, please remember that their goal is to return the computer to some operating state as quickly as possible. They do not care about saving your data. They only care about keeping the computer operating to beyond the end of the warranty period by doing as little as possible.

When the large chain stores repair a computer, they take the quickest approach to complete the repair. This typically means rebuilding Windows®. A quick reinstallation of Windows® is the cheapest repair because it takes about an hour. However in this case all of the customer's data is lost and all the application programs need to be reinstalled. When a customer brings in a computer for this type of repair, it gives the chain stores an opportunity to sell them computer hardware and software that they don't necessarily need. This is the kind of computer service that naïve customers get from large organizations.

Rebuilding Windows®

Rebuilding Windows® is the repair with "extreme prejudice" option. Rebuilding Windows® is typically done as a last resort to remove viruses from your computer. In this book we have presented a virus removal approach that emphasizes saving your data and your programs. However, we go through an escalating procedure as dictated by the problems encountered during the virus removal. When nothing else works, then and only then do we resort to the "ultimate sanction", reinstalling Windows®.

Sometimes rebuilding Windows® is required to make a computer operate properly even though there are no viruses involved. After a computer has run for several years, is a good idea to rebuild Windows® and clean out all the junk and stuff that have accumulated over time. Computers are like my two-car garage that at the time it was built held two cars. However,

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

today no cars fit in the garage because of all the stuff that has been stored there over the last 15 years.

Windows® is the same way. Over the course of several years Windows® tends to accumulate program after program after program. This accumulation of software slows Windows® down and eventually makes it so that it is more frustrating and painful to use the computer than to pound your thumb with a hammer.

Reinstallation Caveats

When rebuilding Windows®, there are several things to remember. First all in many cases the data is wiped off the disk drive. So if you want to save your data, you must copy it to an external disk drive or some location that retains it until can be restored.

Second all of in most cases the programs on your computer must be reinstalled. Reinstallation of Windows® wipes out the Registry entries that are used by programs installed in the computer. That means that those programs must be reinstalled in order to operate as they did prior to installation of Windows®. This is particularly true of Microsoft® programs such as Microsoft® Office.

Some programs are portable programs and may not need to be reinstalled. A few older programs behave in this fashion, and there are newer software programs advertised as portable programs. These programs are installed in a folder that can move from computer to computer. The program runs out of that folder on any Windows® computer.

Finally, installation is different for Windows XP® and Windows 7®. In some cases reinstallation CDs are required. In others Windows® can be restored from a maintenance partition that has been set up on the computers fixed disk drive.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Nerd Tip: *Save every CD or DVD that comes with your Windows computer in a big box. Do not worry about keeping then neat and organized, just save them all. Save the CDs and DVDs that come with purchased software as well. When there is only a printed product key, save it with the CDs and DVDs. As long as this is saved in one location or one big box, when it comes time to rebuild your computer the installation CDs or DVDs and product keys needed will be where you can find them.*

Windows XP® Reinstallation

Windows XP® is the easiest Windows to reinstall. When repairing problems caused by virus infestations, there are two options for reinstalling Windows XP®. The first option is to install Windows XP® right over top of Windows XP. This is a lightweight repair that does not disturb your data and does not require reinstalling your application programs. Installing Windows® over Windows® can straighten out booting, Registry and driver program problems. However, more serious problems require a complete installation of Windows®. The complete installation option wipes the fixed disk drive and installs Windows® from scratch. In this instance all data and programs are wiped from the disk drive.

Most all Windows XP® reinstallations are done by using CDs. Usually the computer manufacturer provides a Windows XP® reinstallation CD. They may also supply other CDs to permit reinstallation of driver programs and ancillary software that came with the computer when it was delivered from the factory. Some computers require you to burn your own reinstallation CDs when you first set up the computer. The reinstallation CD must match the exact version of Windows® that is installed on the computer. In other words, Microsoft® Windows® Home Edition must be installed from a Microsoft® Windows® Home Edition CD and not from a Microsoft® Windows XP® Professional CD. Microsoft Windows XP® Media

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Center edition requires installation using a Microsoft Windows XP® Media Center CD.

Reinstalling Windows® Over Windows®

When reinstalling Windows over Windows® you start by booting from the Windows® installation CD. When the CD is booted, the first screen that appears displays a repair Windows® option. See Figure 5 – 1 Windows XP® Installation Options. This is not the option to choose. It leads me Windows® recovery console and does not install Windows® over Windows®. The option to select in the first screen is install Windows® option. When this is selected, it leads to a subsequent screen that offers both a Windows® repair option and an install Windows® from scratch option. Striking ENTER leads to the second Windows® repair option for installing Windows® over Windows® or to the installation option for installing Windows® from scratch.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

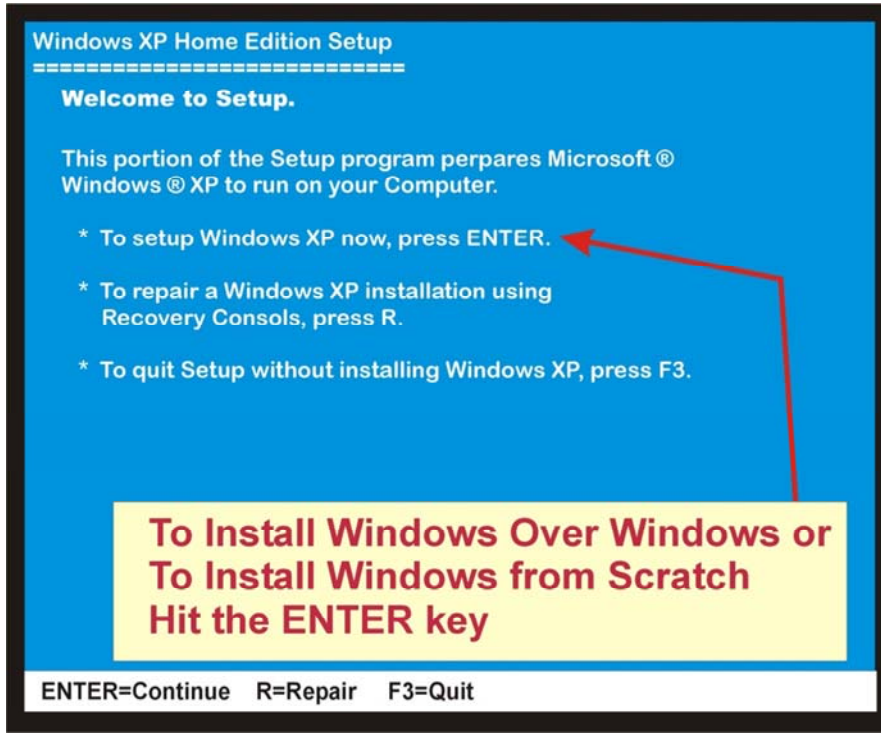


Figure 5 - 1 Windows XP® Installation Options

When the ENTER key is hit, Windows® the Setup program then scans the disk drive for installed versions of Windows®. See Figure 5 – 2 Windows XP® Repair or Replace Options. If the installed version of Windows® matches exactly the Windows® that can be installed from the CD, then the installation software proceeds to reinstall Windows® over Windows®. This reinstallation returns Windows® to the version that is on the CD. If the version of Windows XP® on the CD is a Service Pack 1 version, the computer will now have a Service Pack 1 version of Windows® installed on. You will then need to have Service Pack 2 and Service Pack 3 reinstalled. Additionally, Windows® requires about 100 updates to be installed beyond Service Pack 3. The reinstallation of Windows® and the updates can take hours to complete.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

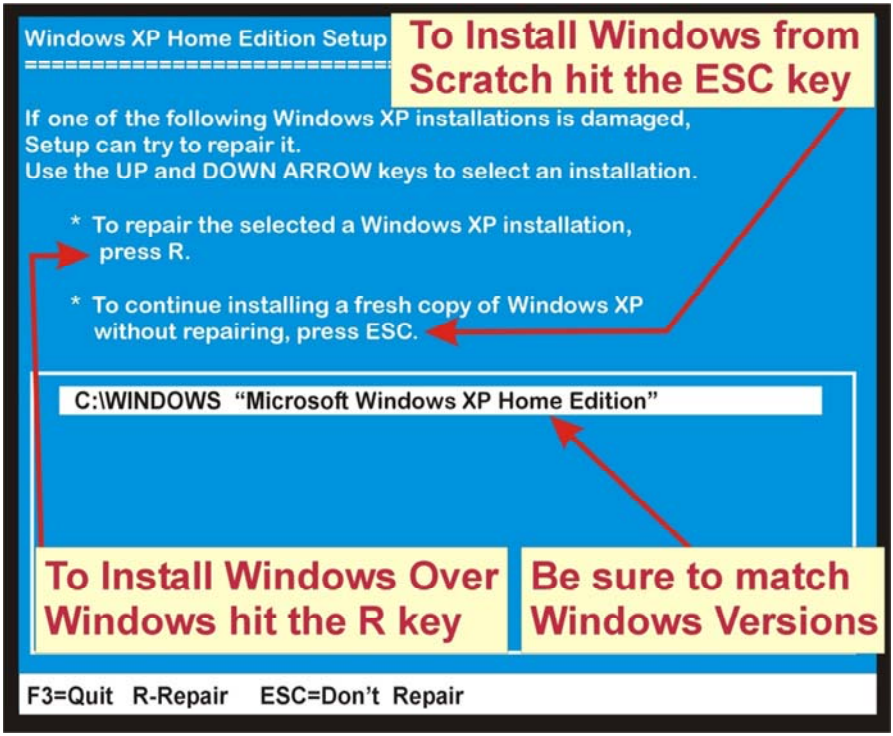


Figure 5 - 2 Windows XP Repair or Replace Options

The success rate of installing Windows® over Windows® and correcting the Windows® corruption problem is about 3 successes out of 10 reinstallation attempts. Although this is a very low success rate, the benefit of installing Windows® over Windows® is that the software settings and set up for all the application programs and the data files are retained on the computer. This means that no reinstallation of the application programs is required. It also means that all of the data remains on the computer and does not need to be copied from some backup location to restore it.

Sometimes during the reinstallation process of installing Windows® over Windows®, errors occur. Please try not to be too concerned about these errors. The main goal is to complete the installation process. If some files are missing, that is likely not preventing Windows® from running properly

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

after installation. Please remember that most Windows® corruption is caused by a corrupted Registry and not files missing from Windows®. Also you have scanned the computer thoroughly so all virus files have been removed from it. This means that when the Windows® over Windows® installation is complete, and your computer runs as you expect, that all viruses have been removed from the computer and you are good to go.

Complete Windows XP® Reinstallation

Choosing installing a fresh copy of Windows XP® is the option for a complete reinstallation of Windows XP®. This option permits you to delete all data on the disk drive, and install a fresh copy of Windows XP®. After the fresh copy of Windows XP® is installed, you need to reinstall all of your application programs and copy your data back to the user accounts. The good news here is that this process is the way to completely remove all remnants of viruses from your computer.

If you first install virus scanning software before you restore the data to the user accounts, the virus scanning software will scan all files that are being copied from an external disk drive to the fresh Windows XP® installation. If there are any virus remnants hidden within the user accounts, copying them with a virus scanner installed permits the virus scanner didn't catch any of the virus remnants. When this procedure is followed, you can be really sure that no viruses remain on your computer.

Nerd Tip: *Sometimes it is possible to restore some old programs by retaining the old copy of Windows® when doing a complete reinstallation of Windows®. Renaming the Windows® folder to Winold and the Documents and Settings folder to DS, allows a fresh copy of Windows XP® to be installed with the old copy of Windows® not erased from the drive. When the windows folder for the fresh copy of Windows® is renamed Winnew and the Winold folder is renamed windows, the computer will boot with the old copy of Windows®. All the programs are still installed in the Program Files folder but they may or may not run because the fresh*

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Windows® installation has replaced the Registry. It is possible to test programs by running them. When a program gives an error saying that it is missing a file (like a DLL file), that file may be found in the Winold/system32 folder. It can then be copied to the Windows/System32 folder to permit the program to run. This is not guaranteed, but it sometimes works.

Windows 7® (or Vista®) Reinstallation

Windows 7® does not permit installing Windows over Windows as a potential Windows repair option. When Windows 7® is seriously corrupted; a complete reinstallation is the only repair option. Windows 7® does provide a boot repair capability. When Windows 7® fails to boot, a boot repair CD can be used to correct the issues that are preventing Windows 7® from booting properly. The boot repair CD is created as part of the Windows 7® installation or initial configuration process. See Figure 5 – 3 Windows 7® System Recovery Options.

Windows 7® Startup (Boot) Repair

The Windows 7® Startup Repair option fixes Windows booting problems. The System Restore function uses the Windows system image gathered from a Windows 7® system restore point to return Windows 7® to be operating state at the time the system restore point was created. When System Restore is not enabled, this type of restoration is not possible. With Windows 7® it is always good to enable the System Restore function. System Image Recovery uses a backup image of the disk drive to repair Windows®. Sense backup images are rarely made; this method of restoring Windows® is rarely available. The remaining two System Recovery Options are used to diagnose computer hardware problems.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

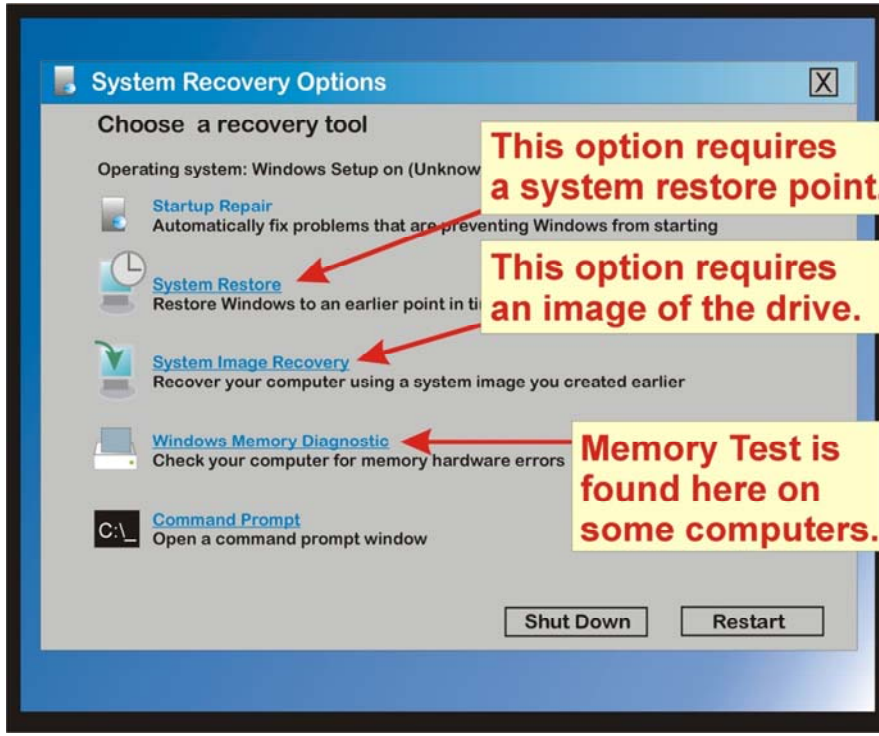


Figure 5 - 3 Windows 7® System Recovery Options

When the Windows® Startup Repair option is chosen, the Startup Repair window opens. See Figure 5 – 4 Windows 7® Startup Repair Window.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

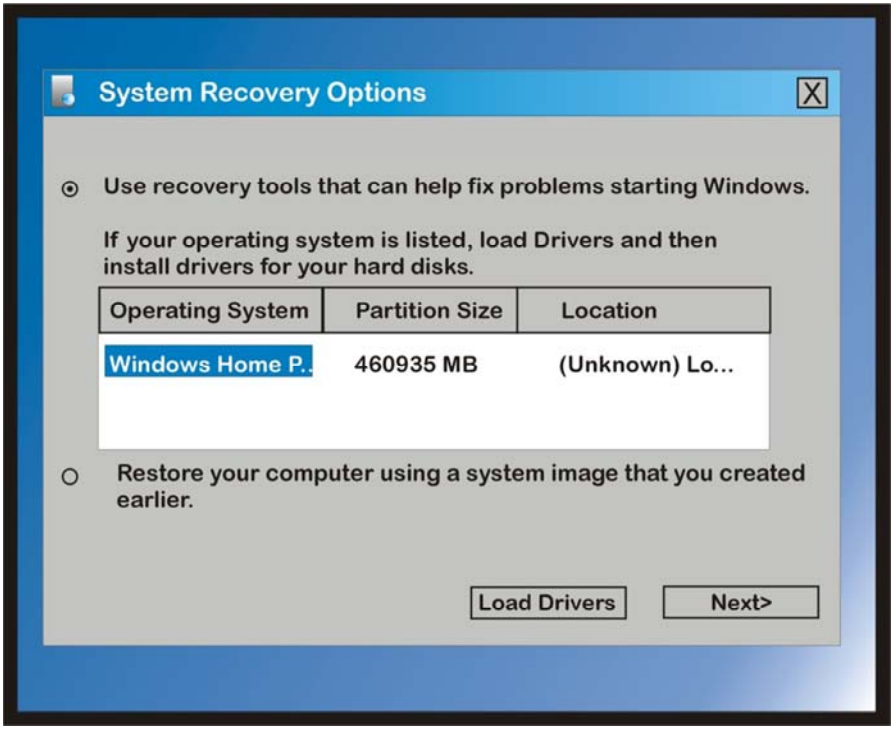


Figure 5 - 4 Windows 7® Startup Repair Window

Windows panel appears, Windows 7® has already searched the disk drive for the Windows installation that requires startup repair. Be sure the installation is highlighted, and then click next to complete the startup repair.

Windows 7® Complete Reinstallation

Many computers have a system maintenance partition installed which permits complete reinstallation of Windows 7® from the computer's disk drive. Since this reinstallation depends upon the disk drive, it is essential to check the disk drive for errors prior to attempting to reinstall Windows® using the maintenance partition.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

When the computer provides complete reinstallation of Windows® by a maintenance partition on the disk drive, that reinstallation is entered through the boot process. The computer has one of the function keys assigned to the system recovery process as shown in Figure 5 – 5 System Recovery Boot Screen.

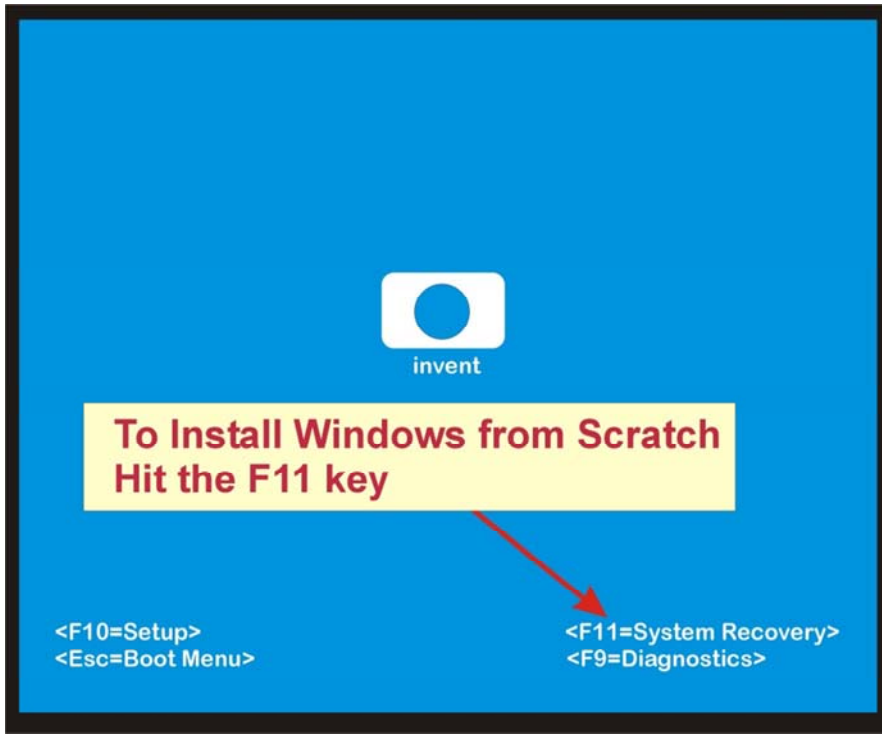


Figure 5 - 5 System Recovery Boot Screen

In our example tapping the F11 key causes the computer to load the system recovery program from the system maintenance partition. These system recovery programs restore the computer to the original factory shipped software configuration. They may also permit backing up the data files prior to restoring the system. When you wish to back up the data files, you would attach a USB disk drive to the computer. After the backup option is selected, the system recovery program then copies all of the

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

data files to a location you designate. In this case you would point it at the external USB disk drive. It can take several hours to save your data. It is probably a good idea to plan on 24 hours of time for the data to be saved in the computer to be restored to its factory shipped software configuration. See Figure 5 – 6 System Recovery Program Options.

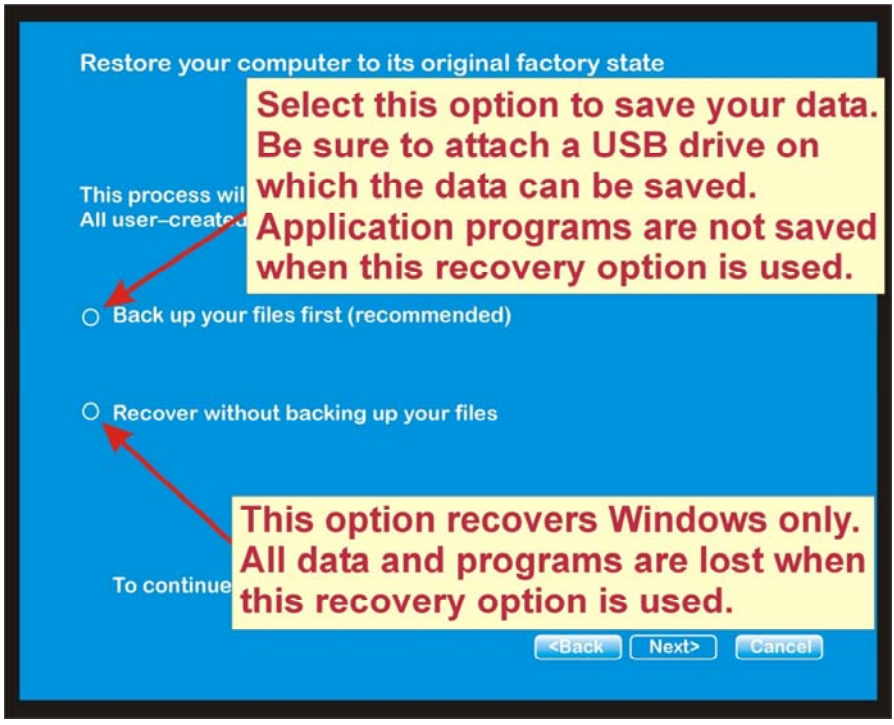


Figure 5 - 6 System Recovery Program Options

Once you give by the initial recovery information screen, there is no turning back. The system recovery program immediately reformats the drive wiping all data from it. In Figure 5 – 7 Recovery Information Screen clicking on the next button immediately starts the system recovery.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Figure 5 - 7 Recovery Information Screen

Rebuilding Windows from scratch provide you an opportunity to really clean up your computer. The most effective procedure for returning your computer to your personal software configuration after Windows has been reinstalled is to install the most important and most use programs immediately. Then in the coming weeks install the remaining programs as the need to use them arises from the work you are doing.

The most important programs to install initially after rebuilding Windows are the office suite software that you use (Microsoft® Office or Open Office.org), web browsers (Mozilla Firefox®, Safari®, or Google Chrome®), and of course virus scanning software (Norton®, McAfee®, Kasperski®, or AVG®). Finally, copying your data from the Users folder to the fresh Windows® installation Users folder completes the process.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Summary

Rebuilding Windows® is the most thorough virus removal procedure. It also dramatically improves the performance of your computer because the junk software that has accumulated over years of use is removed. The quickest and simplest way to remove viruses is to rebuild Windows®. The major drawback is that you must reinstall all of your application programs and copy your data files into the appropriate folders after the Windows® reinstallation is complete. Rebuilding Windows® also requires that all of the Windows® updates must be reinstalled. This includes the major Service Packs. With Windows XP® may need to start by installing Service Pack 1 (SP1) and Service Pack 2 (SP2) and finally Service Pack 3 (SP3) as well as close to 100 updates to Windows® that have been issued set Service Pack 3 (SP3) was released. Both Windows 7® and Windows Vista® have Service Packs and subsequent updates as well.

While rebuilding Windows® seems like a daunting process, it sometimes takes much less effort and time to rebuild Windows® than to scan a computer and remove all viruses. Many a time I have spent 10 to 12 hours removing viruses from a computer when I could have saved the customers data, reinstalled Windows® from scratch, reinstalled the basic software, and restored the data in a matter of three hours.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

CHAPTER 6
Virus Prevention

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Nerd Tales

The thing I like the most being a nerd and working on computers is that it is a people business. Now to be sure most people by the time they call me are very frustrated and angry. This just means that you must give them some slack, because computers can be extremely frustrating. I just cannot wait until we can control them with our thoughts. It would certainly stop me from saying bad words each time the computer does not do exactly what I want it to do. Of course I did flunk typing in high school. Yes, being an uncoordinated nerd did not help. If they gave grades in negative numbers, I would have gotten one. I guess my grade of 30 on the final was a gift from the teacher.

Also nerds are not supposed to write, but here I am. Not too long ago I was helping my neighborhood petition to rebuild the highway access into the neighborhood. I gathered all inputs and wrote them into the petition. The neighbors leading the petition movement felt that one neighbor that had a PhD in English could do the job better. Having a PhD in English is different from writing four technical books and thousands of pages of course notes simple enough for non-technical people to understand. But then again nerds do not get a lot of respect. They also missed the critical point that would motivate the politicians and the MVA to move on the highway access approach. That point was the safety of neighborhood school children. I ended up writing a public letter to the local paper and the politicians that accomplished the goal of moving the MVA and the politicians.

Then there the "Geeks" that come in squads. I guess that is because it takes more than one to do the job. They often practice "Technical Harassment" trying to scare the computer owner into leaving them alone while they remove viruses or repair their computer. As I stated earlier in this book Geeks are circus freaks and Nerds come from Dr. Seuss. So nerds are more people oriented which is why I am a nerd and not a geek.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Nerds also like to explain while we fix whenever anyone wants to listen. Hopefully, I have taken a very dry and important topic and breathed some life into it so that you have a better idea of how remove viruses from your computer.

This is why you should not just rush your computer to the nearest electronics store, call the manufacturer, or call a national geeky computer repair franchise. They treat you like you do not know anything and they know everything. (This is definitely not true.) They keep your computer for a week. They sell you anything and everything that they can because they just want your money. If there is anything wrong after the repair, it is not their problem to fix because it is something new (unrelated to the repair) you have done to the computer.

You would probably be better off hiring the nerdy kid down the street to repair your computer and giving him this book to show him what you want.

Computers and computer service are not hard to understand when they are described in a manner to which we can relate as I explained earlier in the Executive Summary. Every technical person should take the time to explain simply what is happening. They should fix the computer and not try to sell you something. They should explain to you what they have done and what you should do to keep the computer running in the coming months. Doing this it enables you to take better care of your computer. So the purpose of this chapter is to help you keep your computer running after the viruses have been removed and normal computer operation is restored.

Virus Prevention

The most effective and fool proof method to prevent your computer from getting viruses is to never turn on or power up the computer. When the computer is powered off, viruses cannot attack it. This method of virus

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

prevention is highly effective but not very practical. However, one thing that helps is powering off the computer when it is not being used. Powering it off makes the hardware last longer (computer life is measured in Power on Hours) and prevents viruses from doing damage to the computer when is unattended.

No matter what you do or how knowledgeable you are, your computer can be attacked by viruses. As I described in Chapter 1 while looking on line for pictures of Saturn starter switches, I clicked on a link to a web site and was hit by a blackmail virus. The bad four letter words started flying immediately. So there is no absolute and completely effective virus prevention software and procedures. However, there are some things you can do to reduce the chance of virus attack. They are observe the "Rules by Which to Surf", periodically (weekly) clean up your computer, and uninstall unneeded software.

Web Surfing Rules

Following some simple Web Surfing rules can keep your computer virus free.

No Free Lunch

When surfing the Internet and visiting web sites, you should remember:

There is No Free Lunch. There are only a few free things on the Internet. If you find "free" or "helpful" programs, download, and install them, they usually come with embedded malicious software. Sometimes you are warned that installing the free/helpful software is an approval for installing other software that spies on you. If you do not permit the added malicious software to be installed, then the free/helpful software does not work.

Nerd Tip: *The most egregious add-on software installed is web browser tool bars. The ASK.com tool bar seems to be everywhere. It is most*

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

annoying. Every time I spot it attempting to be installed, I uncheck the installation box.

Many truly free programs ask for contributions. When they are helpful like Spybot Search & Destroy®, please contribute. General Public License (GPL) programs like Open Office, Firefox®, Google's Chrome® are good software and are free.

Some free software versions have reduced features, or the key feature is disabled. Recently, I tried a new spyware detection and removal program only to find that the removal part was inoperative unless I paid for the program. Do not bother with these programs because you cannot tell how they work. Only test full featured programs that let you use the full version for a trial period.

Avoid Speed Up Programs

There are Few Programs That Speed Up Windows®. Programs that offer to speed up Windows® use some minute feature that when changed improves Windows® performance. However because these programs often run in the background on your computer, they slow down Windows® as much as they speed it up. The net result is minimal performance gain.

Some programs clean the Registry and speed up Windows®. These programs are not noticeably more effective to a human being in speeding up your computer than free for personal use programs like Advanced System Care®, Glary Utilities®, and the Auslogics® programs available for download at www.download.com.

The best way to speed up a computer is to uninstall unneeded programs and to stop un-needed programs from loading into memory. Sometimes the performance improving programs with fancy names are loaded and inadvertently installed in your computer. Recently, I worked remotely on a customer's computer cleaning it up to speed it up. Nothing seemed to

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

work, until I asked about this one performance enhancing program I had not seen before. When they responded that they did know how it got on their computer because they had not installed it, I removed the program and the computer sped up significantly.

At one time I ran a program that kept Windows® memory organized, stopped memory leaks and performed other performance improving tasks. The program ran constantly. (Notice I used the past tense here.) It cleaned and organized my computer's memory, like a mother cleans and organizes a kid's bedroom. This did not make my computer noticeably faster. I felt satisfied having the cleanest most organized computer memory in Columbia, Maryland but I could do an equally (and perhaps a more) effective job of cleaning my computer memory by shutting the computer down and restarting it. There was no noticeable performance improvement from this program.

The bottom line is do not download and install any programs professing to speed up your computer. The more programs running in the background, the slower and less reliable your computer becomes. Minimize programs loaded at Windows® startup. Keep only programs in memory which are absolutely necessary like the virus scanning programs.

Stop speed launcher programs. They are designed to load specific programs quickly, but running speed launcher programs in memory slows down the entire computer. The difference a speed launcher program makes in loading a specific program is not significant to humans.

In Windows XP® sometimes the virus scanning suites slow down the computer because they really soak up the computer's processing power. This is particularly true when the computer has a small desktop (1 GB of RAM or less). In this case try adding more RAM or employing a virus scanning program alone like AVG® or Kaspersky® antivirus.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Remove All "Evil" Tool Bars

Please Avoid Search Bars or IE Tool Bars. When a search bar is added to your Internet Explorer it filters the content of the Internet you request. Search bars can direct you to sites that they want you to visit. This is like jumping in front of the ticket line for the rock concert. Those sites jump in front of you first because the search bar lets them jump to the front of the line. This may delay you find the information that you truly want or worse yet not permitting you to find the information at all.

The best of Internet Explorer search bars can block popup ads and help you get quickly services provided by the search bar developer. The worst search bar can make it nearly impossible to login to your computer. When encountering a search bar, just remember that most all search bars do not improve your searching. Only search sites like Google®, Yahoo®, and Bing® to search the Internet quickly and effectively.

Clean Up Your Computer Weekly

Virus scanning alone is not sufficient to keep your computer protected from viruses. A single virus scanning software suite like Norton® or McAfee® can be compromised by viruses. One potential customer told me had they had "professional grade" antivirus software so they could not possibly have a virus. Apparently, they believed that the automobile advertisement catch phrase "professional grade" magically protected their computer from virus attack. I am sure that they had good luck with that thought.

A simple weekly cleanup is a good virus prophylactic. Please make a folder on your desktop and label it "Weekly Maintenance". To make a folder point to the desktop, click the right mouse button, select new from the pop-up menu and then select folder. To complete the job please type in the "Weekly Maintenance" name.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Now copy the short cuts for Malwarebytes®, Spybot Search & Destroy®, and your virus scanning program of choice (e.g. AVG® or Kaspersky®) into the folder. If you wish you could add programs from www.download.com like CleanUp (the free version) and Advanced System Care® to the Weekly Maintenance folder.

Then once a week during a slow time, update and run the programs in this folder. In this manner you are assured that the computer has been scanned each week. It is best to update your anti-virus software first prior to running the scans. In this manner it can catch the latest viruses as the other scanning software brings the files into memory for scanning.

Nerd Tip: *Clean up your desktop using a folder called Seldom Used Stuff. Create the folder then drag and drop the icons that are on your desktop that you seldom use into that folder. This does not erase the icons from your computer. Whenever you open the folder the icons are there and the programs can be opened.*

The icons to put into the Seldom Used Stuff are EXE installation files, PDF and DOC files sitting on the desktop, shortcuts to programs that are rarely used, and more.

Set the configuration of all scanning software to perform the most complete and thorough scan. Make sure that no file is overlooked.

Please do not let this become a "diet" approach to virus prevention. A diet approach has you faithfully following a "diet" for the first few weeks or so, then sticking to the diet lapses so that the "diet" ends up becoming "no diet". When little is found by scanning, the weekly scans can become a "monthly scan", then a "every now and then" scan and then finally, "It is an emergency so break the glass and scan now!" scan. Unless the scanning software is maintained and updated, when you get to the emergency scan state, you may need to start all over again and download the latest versions of the scanning software.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Nerd Tip: *Add second opinion virus scans to your Weekly Maintenance folder. Second opinion virus scans are scans performed by Internet sites for free. These sites identify viruses and some remove them. Some second opinion sites are:*

http://www.pandasecurity.com/homeusers/solutions/activescan/?

http://security.symantec.com/sscv6/home.asp?langid=ie&venid=sym&plfid=21&pkj=BEGTXPJZXPUQZNIQWPY

http://housecall.trendmicro.com/

These exact site links can change, but if you go to pandasecurity.com, security.semantec.com or housecall.trendmicro.com you should be able to locate the second opinion virus scanning links.

When one of these sites does not work, then try another. The goal is to get one of these sites to scan your computer for viruses.

A small amount of effort in weekly maintenance goes a long way in keeping your computer virus free.

Uninstall Unneeded and Seldom Used Software

Many computers have bad software on them of which the owners are unaware. This software was installed automatically as they surf the Internet. Often children install games and when they are no longer played, they are left on the computer.

Sometimes trial software is installed unbeknownst to the computer user. It may not be a bad virus, but such trial software typically lurks there just waiting for the opportunity to ask for money.

To keep a computer running smoothly, a periodic review of the installed software should be conducted. Anything that is not being used is a candidate for removal.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Often computer owners do not know what software to remove. The Micorsoft® Netframe, Visual C++. Visual Basic, MSXML, Silverlight, and other support programs are good ones to avoid removing. Similarly, some of the HP programs cause problems when they are removed.

Generally, the HP programs are junk and do little for you. Like the order HP supplies. Who would order supplies from HP at HP's astronomical prices? It is best to get printer cartridges at discount chain stores locally or on-line. For example, the printer cartridges for my HP 1600 color printer cost over $200. This is coincidentally the cost of a brand new HP color printer. Replacement equivalent cartridges were offered on line for $125 a set delivered. If these cartridges mess up the printer, I do not care because then I will just get the new printer. The bottom line is that much of the software that comes with HP printers and computers is of little use to the owner. However, removing it sometimes messes up the computer.

If you need to remove unwanted HP software, uninstall the entire device e.g. the printer then go to the HP web site and just download the drivers for that specific HP printer. Install only the printer drivers and not the other useless software. Sometimes when you install a HP printer using the HP setup program, there is an option to not install the extra useless software. This option is not evident. To find it you must very carefully examine every menu selection during the HP printer installation process.

Sometimes program updates harm the computer. Most Microsoft updates fix security flaws in Windows. These updates are OK. Some driver updates can cause the display to not to work properly. The computer can usually be booted into Safe Mode which uses the most basic Video Graphics Array (VGA) driver programs. Once in Safe Mode the Control Panel can be used to reach the System settings and then the **Device Manager**. Selecting the **Display adapters** permits opening a properties panel with a **Drivers** tab. Selecting the **Drivers** tab reveals a **Roll Back Driver button** that restores

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

the old drivers. Alternatively, using System Restore can also return the computer to operating the way it did prior to the driver update.

A common complaint and belief is that a slow computer is caused by a virus. More often than not a slow computer is caused by computers with 512 MB RAM or less trying to run several memory resident programs at the same time.

On computers with low memory removing memory resident programs of blocking them from loading automatically at Windows® startup, improves performance. Memory under 512 Mb requires constant swapping between the RAM and the disk drive. This dramatically degrades computer performance. When it comes to performance, more RAM memory is always your friend.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Summary

In this chapter we presented three approaches to preventing viruses from attacking your computer in addition to installing and running virus prevention software. Surfing safely reduces the chance of virus attack. Some computers are used for years with no virus scanning programs installed and without getting a virus infection. In this case the computer user only visited a few safe sites like their bank and their email. Computers that are most attacked go to high risk sites like gambling sites, porn sites, software cracking sites, links from social networking sites, and sites offering free stuff.

Weekly maintenance can catch viruses before they have a chance to damage a computer and Windows. Finally, removing unused and unneeded software reduces the chance that a virus can attack your computer.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Conclusion

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Thank you for reading this book. We hope that it has been helpful to you and saved you some money. At the very least you should now understand what constitutes a thorough virus removal.

If you have not been able to successfully remove viruses, please email me dialanerd@verizon.net so that I can make sure you successfully complete the job.

We have tried to make a dry subject somewhat interesting. Although, my nerd humor is sometimes not humorous (except to nerds). Better to smile at a bad joke than to never simile at all.

My soul mate Cate (definitely not a nerd or a technical person at all – you know opposites attract) felt that she could use Chapter 2 and Chapter 3 in cookbook like fashion and be successful to some degree in removing viruses from a computer. Maybe the Nerd in me is beginning to influence her. She is now using some iPhone Apps. Who knows?

The overall approach in Chapters 2 and 3 is complete and the tools are good tools. But like a cook book some of the fine details may be missing (Navy approach Vs. Air force approach).

Also solutions to damage done to your computer by viruses are provided in Chapters 4 and 5. So you have a very good chance of truly removing viruses and restoring your computer to normal operation.

Of course the best defense is a good offense. Preventing viruses in Chapter 6 is that offense, if you follow it.

Publishing this book electronically has been a daunting task. It has been particularly difficult formatting the book for electronic book readers and PC book reading programs. It has taken several weeks to finalize the formatting. The goal is to make it easily readable in multiple formats.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Please tell your friends about this book. Our goal is to help computer users and save them some money. So the more people know about this

book, the more helpful we can be. Also if the response is good, it will encourage me to finish "Pete the Nerd's Do It Yourself Home Network Repair".

Finally, if you like the book, or have any comments please email me at dialanerd@verizon.net.

Thank you again.

Pete
Dial A Nerd

Your Friend on a Technically Challenged Planet ©

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Please Use This for Notes.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

About The Author

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Pete is the original Dial-A-Nerd. The Dial-A-Nerd concept was created in the late 1980's to provide telephone help to the general public. Dial-A-Nerd was originally advertised in the 1990 USA Today classifieds. Dial-A-Pete is the original Dial-A-Nerd. Dial-A-Nerd was created in the late 1980's to support and help to the general public by phone. Dial-A-Nerd's first advertisement appeared in the 1990 USA Today classifieds. Then Dial-A-Nerd Radio show on WJFK Radio and the Technically Correct TV Show on Baltimore's WMAR ABC Channel 2 were created and broadcast.

Pete has worked on computers before the earliest days of personal computers. During his early years working in data communications he personally met some of computer pioneers including Gene Amdahl, Dr. Karl Hammer, Dr. Larry Roberts, and more.

Pete founded The Moulton Company that developed and delivered the first PC Troubleshooting Seminar worldwide. Pete has developed and delivered seminars on Telecommunications, PC Troubleshooting and Repair, and Networking on every continent on the Planet save Antarctica.

Pete wrote several books for Prentice-Hall Publishers including "A+ Certification and PC Repair Guide", "The Telecommunications Survival Guide", and "SOHO Networking."

Pete's PC support and troubleshooting experience comes from building and supporting PCs, and training non-technical users to maintain and troubleshoot PCs over the last 30+ years. His work continues today and has led to writing and publishing "Pete the Nerd's Virus Removal For Everyday Users."

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Disclaimer

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Every effort has been made to verify the accuracy of the material described in this book. However, the copyright holder makes no warranties, expressed or implied, as to the accuracy or freedom from error of this book or the products described in it.

Except when otherwise stated in writing, the copy right holder and/or other parties provide this material as is without warranty of any kind, expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The entire risk as to the quality and performance of the information and recommendations presented is with you. Should the information and recommendations presented not work or destroy data, you assume the cost of all necessary servicing, repair or correction. This is because the copyright holder and/or other parties do not control and monitor how the information and recommendations presented in this book are implemented and used by you.

In no event, unless required by applicable law or agreed to in writing, will any copyright holder, or any other party who may modify and/or utilize the information and recommendations contained in this book be liable to you for damages, including any general, special, incidental or consequential damages arising out of the use or inability to use the information and recommendations (including but not limited to loss of data or data being rendered inaccurate or losses sustained by you or third parties), even if such holder or other party has been advised of the possibility of such damages.

Mention of any product does not constitute an endorsement of the product.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.

Examples are based on real world situations. They have been modified to protect the identity of persons, organizations and companies. Any resemblance to actual persons, organizations, or companies is entirely coincidental.

Copyright © 2011-2012 by Pete Moulton All rights reserved Worldwide.