Empowering Freshmen with Technology Skills: A Security Check Approach

William VanderClock
John T. Gorgone
CIS Department, Bentley College
Waltham, MA 02452-4705, USA

Abstract

When freshman enroll in Fundamentals of Information Systems (IS 2002.1) or Personal Productivity with IS Technology (IS 2002.PO), they have the same attitude as for any other required course: Why am I here? Why do I need to take this course? This paper presents one way in which to change this attitude and, at the same time, teach students about how to use their computer. Freshmen download "stuff", lots of stuff, from the Internet to their computer. Over time, they become paranoid as they encounter hostile spyware, viruses, and worms. They recognize that they need technology skills to be able to maintain and protect their own machine. This paper outlines a strategy for getting freshmen involved in learning about the technology by helping them to overcome their fears. The intent is to capture their interest in information systems by providing the know how to cope with computer software maintenance, Spyware, viruses, worms, Windows updates, disk defrag, disk check and Windows disk clean. The paper describes the process used to gain their interest and includes a handbook that can be used with students everywhere.

Keywords: computer threats, maintenance, teaching the introductory course

1. INTRODUCTION

With the continual growth in required curriculum, many schools, such as ours, combine the required service course (IS2000.2PO) with the discipline introductory course (IS2001). Because students select or are assigned to sections seemingly at random, the students in each class have a broad range of ability, interest, and technology skill. For required courses such as these, students typically don't want to take the class, particularly if they are not interested in (or hostile to) technology. Similarly, many are of the opinion they know enough technology from high school or personal experience and can't conceive the need to know more. Today's students differ from those of the 80's and 90's in that they don't know about a world without computers. Since computers are ubiquitous in their world, they assume they know all they need to know. As teachers, we are faced with the challenge of motivating these students to learn the fundamental concepts of our discipline, information systems.

Although many students are disinterested in the subject in the abstract, they show strong personal concern for "their" computer. Their computer experience is mixed.

1. They love to download "stuff", lots of "stuff" from the Internet and to communicate with their peers and their families via e-mail or instant messaging.
2. Some are skilled enough that they create and maintain their own web pages although their skills are extremely limited.
3. On the dark side, they experience worms, viruses, and other malicious hacks that lead to both fear and loathing of the computer. Their angst is reinforced by reports of denial of service and other security in-

trusions in the press, on TV, and in their college newspaper.

4. They don't know how to defend their computer or even how to maintain what they already have. They panic when they have a computer based assignment and their computer goes down.

This paper introduces one way in which to attempt to change this attitude and, at the same time, teach students about how to use their computer. The authors have tried this technique in their own classes and found it an effective way to motivate students to learn technology skills and to peak their interest in learning more about information systems. Some even become majors.

The authors plan a more formal evaluation using pre- and post- testing to determine the effectiveness of the technique.

At Bentley College, all undergraduates are required to have their own portable computer with Microsoft Windows XP Operating Systems, Microsoft Office XP and specialized software. The authors have approached this paper with the assumption that most college students have access to the Internet and own their own desktop or portable computer using Microsoft XP operating system or have access to a computer for the introductory course and may be interested in buying a computer. Of course, the material presented may be modified to fit different computing environments.

The paper presents the material in the form of two handbooks with the student handbook *Guide To Clean Up A Computer* presented first followed by a handbook for *Selecting a Computer*. This method of communicating is being used in order to facilitate the use of the handbooks in classes. Once into the course, some students will be interested in setting up and maintaining their own home network and this will present an opportunity for an instructor to create another handbook.

The first handbook describes a brief set-up scenario for the student. It then introduces and discusses a series of topics revolving around the theme of cleaning up and maintaining their computer system in today's Internet environment.

2. HANDBOOK GUIDE FOR CLEANING UP A COMPUTER

Almost anyone using a Windows based computer connected to the Internet has run into issues with the machine under-performing. The varieties of things that slow down the computer and get in the way of productivity seem to increase every day. Enabling students to find and repair the problems is a major component of empowering them and interesting them in Information Systems. This handbook walks them through the clean up and maintenance of the computers that they use. Most students are intimidated by the "behind the scenes" part of the software. The handbook takes them systematically through the solutions and removes some of the anxiety in the process. Once they have effected change that makes the computer run better, they gain the confidence to look further into the software and find more solutions.

HANDBOOK: GUIDE TO CLEAN UP A COMPUTER

INTRODUCTION

The computer is a marvelous technology but it has very little hardware or software to protect it from the Internet villains of the world. Malicious hackers assault most Windows based machines when connected to the Internet. The longer it has been on the Internet and the more songs, movies, art work, games, pictures, and software down loaded and installed, the worse the machine's condition may be or will become. You may notice immediate inferior performance or the computer may gradually deteriorate over time and come to a complete lock-up mode. What is sneaking into your computer -- a virus, worm, Spyware, cookie, or Trojan horse? Did your CD-Rom tray open and close without you doing it? Is someone keeping track of each key stroke depressed or web site visited? What should you do? Can you fight back? What can you do to protect your computer? The following is a guide to help you understand the hazardous environment, technology, and what you can do to preserve and protect your computer and work in a more secure Internet computing environment. This is a dynamic document and will need to be updated as the

Internet environment and Microsoft software changes.

HAZARDOUS COMPUTER ENVIRONMENT

A brief word about the hazardous environment we work in. Most computer problems people experience result from poorly written software, inadequate operating systems and outsiders trying to either take control of your computer or plant malicious programs in it or suck information out. The most common types of malware are viruses, worms, Trojan horses, cookies, key logger and Spyware and they are everyday occurrences. A virus is a computer program designed to replicate and take actions on your computer without your permission. Worms are similar to viruses but designed to spread over network connections. They exploit known security flaws and spread quickly through networks leaving a trail of damage. A Trojan horse, just like the Greek story, opens the doors protecting your computer at the worst possible times. A cookie can be used improperly by a Web site can send back information about sites you visit and share the information filled out at the visited sites with others. Small programs that send information about the computer and its user(s) to marketers is know as Spyware. Spyware programs often clash with legitimate programs on the computer. Key Logger is a device that records keystrokes. Using this, the owner can collect usernames and passwords from anyone who uses the computer. A back door is a way to by-pass security like user names and passwords using computer software. These are things that can happen to your computer.

PROTECTIVE ACTION – BE PROACTIVE

What can you do to protect your computer environment? First, stay alert! Don't open suspicious looking email or email attachments. Any legitimate email attachment should be scanned with your anti-virus package before opening it. Don't blindly check the "I agree" statement at the bottom of the license agreement conditions agreement for downloading and using the software.

Investigate before you add new programs. You sometimes get more than you wanted, especially with free programs. A little time spent looking up the program and checking what more than one source says about it may help you avoid adding something to your computer that brings spyware along with the program. Next, the paper presents the options and methods that can be taken to preserve and project the computer you are working with to provide a more secure computing environment.

RE-IMAGE YOUR COMPUTER

Most computer manufacturers supply disks that will return the computer to its original state. The computer's hard drive will be completely cleaned off and the original software provided by the computer manufacturer will be reinstalled on the machine. Your computer will never run better than it does with that original image as the *only* software on the machine. The advantage to this approach is a fast, no cost, easy fix to all software problems. It fixes everything except hardware problems. The disadvantage to this method is that you lose all data and other software not backed up somewhere else. Software not on the computer when you purchased it must be reinstalled, either through new downloads from the Internet or from the original disks. Any software settings will be lost along with all Favorites contents in Microsoft Internet Explorer. This method returns your computer to the way it was when it came out of the box.

To re-image your computer, find the disks supplied by the manufacturer and follow the manufacturer's instructions. Most manufacturers have hot-line numbers and helping someone through re-imaging is relatively easy for them to do. Make sure you back up anything that you need from the computer *before* you start the process.

CLEAN IT UP YOURSELF

This option can be a 7/7 undertaking. That is, it takes from seven hours to seven days of work to complete. There are no guarantees of success but if these measures fail, one can go back to the re-imaging solution.

Step 1 – Get rid of the viruses/worms: Unless you have been scanning your computer drives at a minimum of once a week with two different scanners, there is a very good chance you have a virus, worm and/or Trojan horse buried in your software. First,

start by scanning from the outside with a Web scanner.

1. A favorite can be found at http://housecall.trendmicro.com .
2. Scan your entire hard drive with this scanner. The web site will direct you to a one-time download of a small client that makes this Web scan possible.
3. Anything that the Web scan finds and did not clean up will be on a report that displays when the scan is done.
4. Make note of anything it finds on paper.

Second, do a clean scan using the antivirus program that came installed on your machine.

1. Get the latest update to the program that can be done by opening the program and clicking on the update button while connected to the Internet.
2. Once this is complete, shut the computer down and disconnect any wired network connections.
3. Now start the computer and after the BIOS has loaded but before any part of Windows shows up on the screen, press the F8 function key at the top of your keyboard. A menu should appear.
4. Choose the SAFE MODE choice. This will load Windows but without the drivers and start-up software that normally loads. The screen will look funny because it is using generic, low resolution video drivers to paint the screen. Windows will also make sure that you know it is in SAFE MODE by making you acknowledge it and putting a reminder in all four corners of the screen.
5. Click on START and PROGRAMS. Select and click on the antivirus client.
6. Click on whatever does a scan of the C: drive. The scan should take about 20 minutes or longer depending on the size of the C-drive. Wait for it to finish. Nothing else should be done on the machine while the scan is running.
7. Anything the antivirus software finds will appear in a report when it terminates. The program should indicate that it fixed, deleted or quarantined any viruses or worms that it found.

If you identified any viruses or worms that could not be cleaned, deleted or quarantined, you need to seek professional help to remove the virus or worm.

Step 2 – Get rid of the Spyware

Many free programs also contain Spyware as part of the down load and installation process. There is code on many web sites that add Spyware to your computer when you visit the web site. Fortunately, the best tool is a free software program called Ad-Aware SE from Lavasoft. This program is available from a wide variety of web site sources including ZDnet (*http://downloads-zdnet.com*) and Twocows. A Google search will take you to the most current ones.

1. Download the program and install it on the computer. It should place an icon on your desktop that looks like a red circle with a slash through it.
2. Double click the icon and the Ad-Aware SE window should open.
3. On the lower right, just above the start button there is a link labeled "Check for updates now". Click on the link and then click on the connect button. This will go out to the Internet and look for updates that, just like the antivirus program, are critical to the removal of the newest forms of spyware.
4. If an update is available, make sure you get it.
5. Regardless, run the program by clicking on the start button in Ad-Aware SE and then the next button. The Ad-Aware scan goes much more quickly than the anti-virus scan.
6. When the scan finishes, all of the items in the "objects recognized" field are pieces of Spyware that Ad-Aware has identified and will remove for you. Everything listed should be checked.
7. If not, right click on one of them and click on "select all". Follow the instructions to remove them all from your system.

As with the anti-virus software, regular weekly scans are required to keep your computer Spyware free.

Step 3 - Get rid of the old, discarded software.

Most individuals add a variety of software to their computers. Some programs are very

useful and would be reinstalled if you acquired a new computer. Others may not have been used for months and can be removed to improve your computer's performance.

1. Open the Control Panel and click on Add or Remove Programs. You will get a list of programs installed on the computer along with some information about how often you use it.
2. Analyze the list very carefully and remove the software that you installed but don't use. If you are not sure what a program is or why it's on the machine you should probably leave it alone.
3. You will (or should) see a long list of programs listed as "Windows XP Hotfix". Don't remove these, they are updates to your operating system and belong there.

It's a good idea to review the list every couple of months and remove anything you have added but are not using.

Step 4 - **Cleanup the hard drive and get rid of the Temporary Internet files**

Everyone's hard drive gets messy in ways you can't see as a normal part of the way Windows works. The following procedures will clean it up. Doing this task weekly will keep your machine running smoothly and minimize the time the procedure takes.

A. Disk Cleanup

1. Go to My Computer and right click on the C drive. You will get a map of the computer's hard drive showing how the drive's space is being used.
2. There is a button labeled "Disk Cleanup" and you click on that button.
3. After some searching (if you have not done this for a while, it will probably take 10 minutes or so) you will get a list of files that Windows thinks you do not need. In most cases they are correct but check the list carefully.
4. Do *not* check the box for "Compress old files". Temporary files and Temporary Internet files should be checked.
5. After checking off the boxes you want, click on OK to get rid of the files.

B. Check Disk

1. Go to My Computer and right click on the C drive. You will get a map of the computer's hard drive showing how the drive's space is being used.
2. Click on the Tools tab at the top of the Properties window.
3. Click on the "Check Now" button of the error checking section.
4. There are two options on the Check Disk Drive window that opens. Checking either of these will give you a message indicating that neither of these can take place because Windows is using the disk. It does give you the option to do them on the next boot but keep in mind that this could turn the next boot into a multi-hour process.
5. For now, just run the check without either of the options checked. If you do find errors then go back and do it again with the "Automatically fix file system errors" option checked.
6. The un-optioned check will take a few minutes to run and should come up error free. If errors are reported, check the automatic fix option and say yes when it talks about doing it at the next start-up. If the errors are not resolved, take your computer to a computer professional.

C. Defragment

1. This step has the greatest potential for speeding up your machine.
2. Go to My Computer and right click on the C drive. You will get a map of the computer's hard drive showing how the drive's space is being used.
3. Click on the Tools tab, the second section deals with defragmentation.
4. Click on the Defragment Now button. This will open the Disk Defragmenter window.
5. Next click on the defragment button and watch the colored lines change in the "after" window.
6. Defragmenting works much faster if done often. The first time you run it, the time required to finish may be several hours. You should not do other things on your computer while the defragmenter is running.

Step 5 – **Get rid of anything you can in the Notification area of the Taskbar.**

The taskbar at the bottom of your screen shows any open or minimized windows. The area to the right with the time is the Notification area. Every icon located there represents a program that uses scarce resources regardless of whether you actually use the program. Many of these you want and need but do not need them to start every time you start the machine. Quicktime is a good

example of an icon the shows up in the Notification area. Everyone should have Quicktime on their computer and it will automatically open if you double click on a Quicktime movie. You can also click on Start, Programs, and select Quicktime to open the program. You do not need the Quicktime icon in the Notification area. Removing the icon from the Notification area will not affect the program or it's functionality on your computer. To remove most icons from the Notification area do the following:

1. Right click on the icon. If they are "good" programs, you will have several choices that come up on a menu. The last choice on the menu, usually EXIT, will temporarily remove the icon from the Notification area. As soon as you restart the computer the icon will be back. This is a good way to test if you really need the program.
2. Click on exit and see if you miss having it there. If not, you can probably remove it permanently.
3. To remove it permanently, right click the icon and click on preferences or options (each program is a little different).
4. You should find a check-off box labeled something like "Launch Automatically when Windows starts". Remove the check and you should be all set.
5. Unfortunately not all programs play by the rules and you will find some that don't give you a menu when you right click on them. These will require a little more work to get out of the Notification area. Usually opening the program from the Start, Programs menu and looking for preferences or options will lead you to a place where you can change it so that it doesn't load up every time you start the computer.

Keep in mind that there are several programs that everyone *should* have in the Notification area. The anti-virus program, the sound volume control, the local area connections icon(s), the battery icon and the Safely Remove Hardware icons all belong in the Notification area.

Step 6 – Update Windows

All Windows operating systems are very complex and are full of bugs, open doors and other problems. Microsoft provides software updates on their web site for free downloading. To review what is available, do the following.

1. With an Internet connection, launch the Microsoft Internet Explorer Browser. Click on Tools and Windows Update or go to http://v4.windowsupdate.microsoft.com/en/default.asp
2. Click on "Scan for updates". You may get a security window asking if it's OK to load a file from Microsoft. Click on yes if this window comes up.
3. When it has finished checking your computer it will come up with the three update categories, Critical Updates and Service Packs, Windows (version), and Driver Updates. Although Microsoft has its share of problems, the critical updates to the operating system are very safe and highly recommended. Occasionally there will be a problem when these are installed but in most cases the Critical Updates should be installed as soon as they are released.
    a. Service Packs do not have the same safe reputation. Windows XP Service Pack 1 (SP1) had some software issues when first released. It has been fixed and is currently safe to install. Service Pack 2 (SP 2) is causing problems and Microsoft has delayed the automatic installation for several months. The authors recommend waiting at least 2 months after release before installing any Service Pack. See the following URL for more information on Service Pack 1. http://www.smartcomputing.com/editorial/article.asp?article=articles/2004/s1507/37s07/37s07.asp&articleid=20625&guid=9AAEC48C84A84EDF92C37FA53F1E1EFE
    b. Windows (version) is the second category. It includes both recommended and optional updates to the operating system. Most updates are for subsystems such as the Windows Media Player or for foreign language additions to Windows. Read through the list and only accept recommended updates and those that apply to software you are actually using.
    c. The third category is Driver Updates. Microsoft is trying to help users keep up with driver updates. This requires

coordination between Microsoft and the hardware manufacturers. If a driver update shows up on the list for your machine, it is best to check the manufacturer's Web site and read as much as you can about the update before applying it to your machine. Some of these updates you want, others you do not. In Windows XP you have the ability to roll back drivers to previous versions if the new ones cause problems.

4. Click on the button to download Critical Updates and install them. Most of the updates require that you reboot your machine after they are installed.
5. Review and select updates in the other categories as needed.
6. When you are finished with the updates, go out to the Web site again and make sure that the software you installed made computer eligible for additional updates.

ADDITIONAL PROTECTION

There are additional security measures one can adopt to provide a more secure computing environment as well as provide an insight and perhaps better understanding of what is taking place within the network connection. Two security procedures are installing firewalls and routers. A firewall is an excellent way to increase security. Firewalls can be either software, hardware, or a combination of both. Windows XP includes a built-in firewall that can be turned on or off (current default is off) based upon instructions found at: http://support.microsoft.com/default.aspx?scid=kb;en-us;283673&Product=winxp

Briefly, to enable Internet Connection Firewall in Windows XP do the following steps.

1. You must be logged on as an administrator. Click *Start,* click *Control Panel*, and then double-click *Network Connections.*
2. Click the Dial-up, LAN or High-Speed Internet connection that you want to protect, and then, under *Network Tasks*, click *Change settings of this connection*.
3. On the *Advanced* tab, under *Internet Connection* Firewall, select: To enable Internet Connection Firewall (ICF), select the *Protect my computer and network by limiting or preventing access to this computer from the Internet* check box.
4. Click OK

There are also several non-Microsoft personal firewall software packages available, some are free. For example, ZoneAlarm at http://www.zonelabs.com/store/content/catalog/products/sku_list_za.jsp or BlackIce at http://www.digitalriver.com/dr/v2/ec_dynamic.main?SP=1&PN=10&sid=26412.

A second security measure is to install a router. In addition to allowing multiple computers connections to a single broadband modem (cable, DSL, satellite) connection, routers provide an extra layer of protection for computers by using its IP address instead of the IP addresses of the computers connected to it. Most routers designed for home networks use network address translation (NAT). NAT is designed to allow the home user to have multiple machines connected to the Internet and only uses one IP address, the routers. A by-product of this is that NAT creates a barrier that hides the machines using that single IP address, thereby giving each machine additional protection from hackers who use IP addresses. If you spend a little more on the router and get one with a built-in firewall, you get even more protection such as Netgear RP614: http://www.netgear.com/products/details/RP614.php?view=hm or a D-Link DFL300: http://www.dlink.com/products/?pid=66.

A few words about installing wireless routers are discussed next. In most cases, the addition of a wireless router actually makes the computer less protected. Wireless security is not what it should be and placing data on the airwaves makes it fairly easy for someone to "tap in". Even with NAT, wireless routers open opportunities for outsiders to get inside. The old wireless security scheme, Wire Equivalent Privacy (WEP) was almost useless. The newer scheme, Wi-Fi Protected Access (WPA) has the potential to provide the protection required but its implementation has been slow and inconsistent (see http://www.drizzle.com/~aboba/IEEE/ and http://www.iss.net/wireless/WLAN_FAQ.php).

KEEP YOUR COMPUTER RUNNING WELL

Regardless of how you get your computer cleaned up, once you have it working correctly, you want to keep it that way. The following is a list of the tools you should run on a weekly basis to keep the machine running fast and with a minimum of software issues.

Daily

- □ Backup software or date, etc. that you have created or changed to a CD-Rom, floppy disk, or a network drive.

Weekly

- □ Update and run a virus scan of all your hard drives. (antivirus of your choice)
- □ Update and run a spyware scan of your hard drive. (Ad-Aware 6)
- □ Run a disk clean of your hard drive (Windows disk clean)
- □ Run an error-check on your hard drive (Windows disk check)
- □ Run a defrag of your hard drive (Windows defrag)
- □ Check Windows Update for critical updates

Monthly

- □ Check the programs installed and remove the ones you are not using (Control Panel, Add or remove software)
- □ Remove icons from the Notification area of the Task bar for anything that should not be there

3. HANDBOOK GUIDE FOR SELECTING A COMPUTER

Once all the material and exercises have been completed in the Guide for Computer Users handbook, the students are usually ready and interested in knowing how to select a computer on their own. At this stage we give a simple assignment on "Buying a New Computer." They seem to really enjoy the exercise. Notice that we don't assign a specific format for the report. We let them create it on their own and side-step and questions regarding report format issues. Then, after the assignment is completed, graded and returned, we use the opportunity to have a classroom discussion of an "ideal" format. The students enjoy contributing to the discussion and they learn more about specifications and targeting the client's requirements. The following handbook has been prepared for use as a classroom assignment.

HANDBOOK: SELECTING A COMPUTER

This assignment requires you to research and select a computer for an individual. The purpose of this assignment is to match the user's requirements to a computer. Keep in mind that there is no perfect answer, but you will need to be able to justify your selection. Simply selecting a top-of-the-line computer and saying "because it's the best" isn't enough! You should also select basic options as needed. Note that your budget is fixed and you cannot exceed this amount!

For each computer you choose, list the following information:

1. Website or store where you found the sales information
2. Brand
3. Model
4. Price
5. Processor Type
6. Processor Speed
7. Memory Type
8. Memory Size
9. Operating System
10. Additional Equipment/Features

Go to the following websites (Compaq, Dell, Gateway, IBM, Toshiba, or PcsForEveryone.Com) and configure a computer that would meet the shopper's needs. Write a short 2-3 page paper that justifies the recommended selection you made and indicate how it meets the requirements. Explain why this computer is a good fit for the shopper. You can recommend more than one computer if you think they meet the shopper's requirements. You can rank-order up to three recommendations but you must justify each one.

Your client is Samantha James and her budget is $2,300.

Samantha is a web developer and programmer consultant. She travels a lot and needs a lightweight portable computer. She also uses the following applications in her consulting business: email, Internet, Word, spreadsheets, presentations and photos. She stays in hotels when she travels and needs

network access via broadband and analog phone. She also needs wireless access in airports and coffee shops. She uses a PDA and syncs her schedule with her the computer. Since she travels back and forth, from Europe and the USA she needs a long battery life of at least 4 hours to work on the airplane and watch DVD movies. She needs the ability to back-up files on CDs. She needs a powerful machine that is capable of running advanced software with minimum of 512MB of memory. This computer will also serve as her home machine where she has an "old" LaserJet printer with a parallel port and other USB peripherals.

Two months after she buys the computer she will have an additional $500 budget available to purchase hardware upgrades that will improve the computer performance or add additional peripherals. What hardware upgrades or additional peripherals can you recommend to her? Provide your reasons.

4. CONCLUSIONS

This paper provides a strategy to motivate freshmen to learn computer technology and reveals how to use their computer effectively. The intent of the strategy is to capture their interest in the computer discipline by providing the know how to cope with computer software maintenance, Spyware, viruses, worms, Windows updates, disk defrag, disk check and Windows disk clean. In implementing the strategy, it empowers the student to deal with computer technology problems head on and provides the self-confidence to work in a hazardous networking environment. The tools presented in the paper help raise the interest level of the student and provide the motivation to pay attention to information systems as a discipline. You are encouraged to use these tools to empower and motivate your students. The important thing is to expose students to new ideas and solid information that will lead them into a future that embraces technology regardless of their specific interests.