Project Number: 12-03 HNH014

Microsoft Toolkit and Social Implications

An Interactive Qualifying Project Report

submitted to the Faculty

of the

WORCESTER POLYTECHNIC INSTITUTE

in partial fulfillment of the requirements for the

Degree of Bachelor of Science

by

Deshawn Fentress

Deshawn Fentress

Colin Pacelli

Colin Pacelli

Date: May 3, 2004

huong higgins

Professor Huong Higgins, Major Advisor

Abstract.

The goal of this report is to investigate public awareness of worms and viruses in order to draw meaningful conclusions about what type of people contact viruses and what actions make these people vulnerable. By using survey results, this investigation will link types of computer users to rate of virus infection. The discussion will prove that there is a strong correlation between unskilled computer users and their high rate of virus infection. The survey and analysis will give insight to security measures people can use to prevent infection.

Table of Contents

Authorship Page

1. Introduction	Colin
2. Review	
2.1 Sapphire/Slammer Worm	Deshawn
2.2 Microsoft SQL Critical Update Kit	Deshawn
2.3 SQL Critical Update Kit	Deshawn
2.4 SQL Scan	Deshawn
2.5 SQL Check	Deshawn
3. Methodology	Deshawn
3.1 Strategy	Deshawn
3.2 Three Goals of the Project	Deshawn
3.3 Survey Design Method	Colin
3.3.1 Establish Goals	Deshawn
3.3.2 Determine Sample	Deshawn
3.3.3 Choosing an Interview Method	Deshawn
3.3.4 Creating the Survey	Deshawn
3.4 Getting the Survey Out	Colin
4. Survey Results and Analysis	All
5. Conclusion	
5.1 Discussion	Colin
5.2 Experimental Errors	Colin
5.3 Summary	Colin
6. Bibliography	All
7. Appendices	
Appendix A: Survey	All
Appendix B: Results Spreadsheet	All

1. Introduction

Today, the Internet is recognized and accepted as a global social institution. It has become a vital part of day to day life for the entire world. From stock traders, political correspondence, or the transfer of security information, to online gaming or advertising, the Internet is a dynamic, yet omni-present, establishment in one capacity or another. Because the Internet is widely used, internet security is important. Yet, commonly used products come with security flaws, and these flaws can be detrimental to society as there is growing dependence on the Internet. This investigation will also educate internet users.

By considering survey results, a level of virus susceptibility can be assigned to each genre of computer users. This will make people realize their own risks to virus infection and encourage them to improve their computer abilities.

In order to further educate partakers, many survey questions have introductory information about the topic in the question. To answer the question properly, survey takers will have had to read and understand this information.

The three main objectives of this study are figure out which genre of users is more susceptible to worm infections, discuss the Toolkit and share and provide information about it, and investigate public awareness of worm and virus information. A user is more likely to avoid viruses if s/he is well-informed about simple preventative measures.

A survey was designed to poll public affliction of the Slammer (or Sapphire) Worm. Findings will prove a correlation between experience of computer use and level of virus infection. By categorizing genres of computer users, labels can be applied to those of higher risk to infection. Studying the trend of association between computer skill and rate of virus infection will give insight in to how help people prevent infection on their own. Global virus proliferation could slow as less and less people share infected files because they know simple remedies and preventive techniques.

The survey was administered via mass email, personal interviews, and group distribution. In filling out the survey, survey takers will discover any weaknesses in knowledge about the Microsoft toolkit and become able to use said information to overcome any vulnerabilities. The survey was administered via mass email, personal interviews, and group distribution. Analysis of results will both shed light onto this subject and also spark innovation in the field of security software.

2. Review

2.1 Sapphire/Slammer Worm

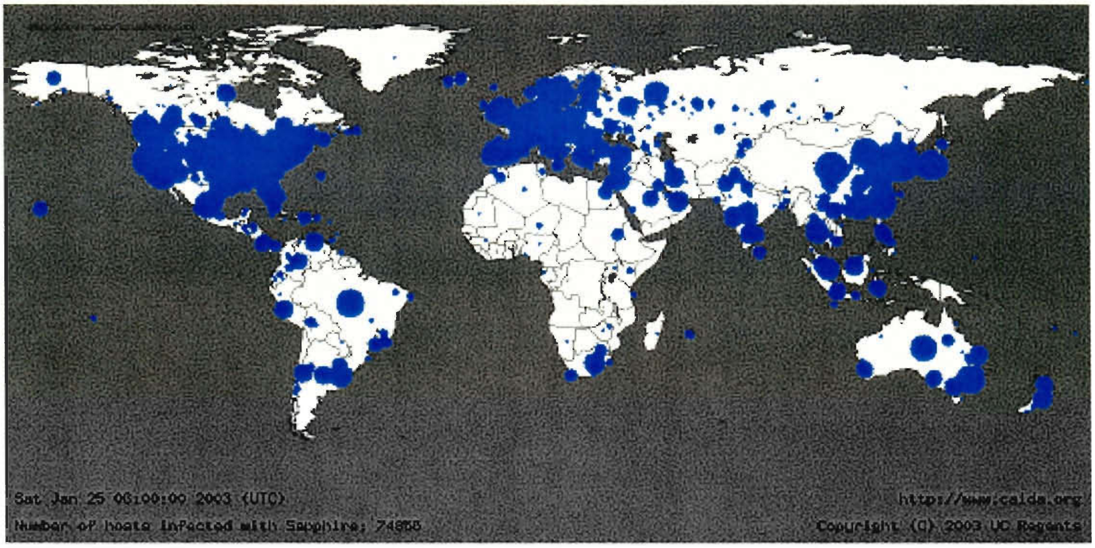
The two most common names for the computer worm is the Sapphire or Slammer worm. The worm has also been refereed to as the SQL Hell. The technical name for the worm is W32.SQLExp.Worm, DDOS_SQLP1434.A or W32/SQLSlammer.worm.

This computer worm began to infect susceptible hosts close to 5:30 AM on Saturday, January 25, 2003. The worm had the capability to detect vulnerabilities on computers using the Internet that were running the Microsoft SQL Server or MSDE 2000 (Microsoft SQL Server Desktop Engine). The main vulnerability was a buffer overflow that the worm would exploit causing a large amount of internet traffic.

The computer worm was operating under a strategy known as random scanning. The worm would select random IP addresses on infect until a susceptible host was located. The worm's unsystematic approach caused it to come across hosts already infected or immune to its effects causing the rapid growth to decrease.

The Sapphire worm has been documented as the fastest computer worm in history. The worm would spread from host to host by doubling its size every 8.5 seconds. The next fastest worm was the Code Red worm which infected 359,000 hosts on July 19, 2001. The Code Red worm's doubling time was about 37 minutes. Over 10 minutes, the Sapphire worm had infected over 90 percent of all vulnerable hosts. The worm infected a little more than 75,000 hosts and caused network outages. **Figure 1** shows the spread of the worm after being released for 30 minutes. After approximately 3 minutes the worm had reached its full scanning rate of over 55 million scans per second. Not too long after the growth rate began to significantly decrease because a number of networks were not able to support the amount of bandwidth.

Fig. 1.1 Sapphire Worm infection


Sat Jan 25 06:00:00 2003 (UTC)
Number of hosts infected with Sapphire: 74855
http://www.caida.org
Copyright (C) 2003 UC Regents

The Sapphire worm was successful in overloading networks and taking database servers offline. The actual amount of destruction does not compare to the amount of propagation received by the worm. If the worm targeted more popular services or attacked a more widespread vulnerability, then the effects would have been more severe.

The characteristics of the worm are what made it one of the most memorable worms to infect computers. The worm had four unique qualities that let it stand out from other worms. These characteristics include: the UDP (User Datagram Protocol) packets, size being small, database infector and memory resident.

There are two data types commonly used on the Internet, the TCP (Transmission Control Protocol) and UDP. The Sapphire worm used the UDP packet because it could be sent and forgotten. To clarify, the worm could be sent to numerous random addresses without actually receiving a reply message. This caused the alarming doubling rate of 8.5 seconds to computers and large amount of network traffic.

The worm is very small compared to most worms or viruses. It is approximately 376 bytes of assembly code. This one package of data acts as a probe and infector as it streamlines through the Internet search for susceptible hosts.

The inventor of this worm could have caused a great deal of damage since the worm infected databases, but the inventor did not focus on such servers. Sapphire was not a malevolent infection considering how much damage it could have carried with it. Despite the viciousness of its ability to scan, the virus did not have severe lasting affects on infected networks. It was rather an annoyance, albeit a large and destructive one. The Sapphire worm is the first computer worm to infect SQL databases on a very extensive scale. The majority of worms attack public targets like web servers and PC hard drives.

Another key function of the Sapphire worm was that it was memory resident. The worm stayed on the main memory or RAM (Random Access Memory) as compared to other worms that copy files to the hard disk. The worm was able to execute so quickly because it was on the RAM but it could be easily erased by shutting down the system because data in the main memory doesn't persist without power.

2.2 Microsoft SQL Critical Update Kit

The SQL Critical Update Kit is a consolidation of three different tools that Microsoft provides for detecting and combating server vulnerabilities. The three tools include: SQL Server 2000 SQL Scan, SQL Check, and SQL Critical Update Kit. The combination of these tools is useful in updating the SQL Server 2000 and MSDE 2000 sections that are vulnerable to the "Slammer Worm".

2.3 SQL Critical Update

This SQL Critical Update tool scans the user's computer for vulnerabilities caused by the Slammer worm and then updates these files. The Critical Update tool searches for instances on the SQL Server 2000 and MSDE 2000 soft wares. The tool is compatible with Windows 98, Windows ME, Windows NT 4.0, Windows 2000 and Windows XP.

2.4 SQL Scan

This function has a different "search and update" procedure when combating the Slammer worm. The SQL Scan tool scans an individual computer's input which is its domain, a range of IP addresses or a single machine name. The Scan tool only identifies SQL Server instances but does not disable, update or repair them. After the Scan tool locates the instance, the problems must be disabling or shut down manually. The tool is compatible with Windows 2000 or higher. It can also identify instances running on Windows NT 4.0, Windows 2000 or Windows XP (Professional).

2.5 SQL Check

The SQL Check tool scans computers for the server vulnerabilities caused by the Slammer worm. The Check tool identifies vulnerable SQL Server 2000 clusters, but does not have the ability to immobilize them. For computers running the Windows NT 4.0, Windows 2000 and Windows XP, the SQL Check tool can stop and disable the SQL Server and SQL Agent services. For computers running the Windows 98 and Windows ME, the SQL Check tool can only identify the vulnerable instance but does not have the ability to fix the problem.

3. Methodology

This Interactive Qualifying Project has been designed to discuss the Microsoft SQL Toolkit and its social implications. The initial task was to design a survey to address three different goals and retrieve qualitative feedback from a target population while simultaneously informing the audience about the Microsoft Toolkit and how it could be used to combat a virus that affects society in the way the Slammer/Sapphire worm did. These respondents classify themselves as WPI students, WPI faculty, WPI staff, business consultants, high school students or other. To analyze the survey better, our target population was separated into two main groups: college students and the inclusive population. The college students consist of Worcester Polytechnic Institute students and users who distinguished themselves as other college students in the survey. The inclusive population consists of every respondent who did not label themselves as a college student. Distinguishing the two groups proved that one received more virus infections.

3.1 Strategy

The users extracted from the surveyed population have been separated into two main groups for comparison and data analysis. These two groups are the college students and inclusive population.

By separating the respondents into two main groups we were able to compare and contrast important data inputted into a number of graphs to determine a conclusion. We developed charts to portray the differences between college students and the inclusive population. The differences graphed are the percentage of users who lack computer course experience and the amount of users affected by a worm or virus based if they were a college student or part of the inclusive population. We also developed pie charts to portray information about the two groups including: the computer literacy rate, frequency of downloads, computer usage and how much the survey increased the knowledge. We felt these types of graphs are easily understood in reporting and could provide qualitative information for analysis.

3.2 Three Goals of the Project

The first goal of the project was to figure out which genre of users is filling out the survey to determine which group of users are more susceptible, college students or the inclusive population. This group of questions helps to determine what actions the respondents are taken that may make them more susceptible. The project developed seven questions to retrieve this information from the population. **(Appendix A)** The first question was designed to determine if the participant was a WPI student, WPI faculty, business consultant, high school student or other type of individual taking the survey. The next question was derived to understand the individual's computer literacy. The surveyed population would rate themselves on a scale from 1 to 5, 1 being a novice user and 5 being a computer expert. This question was followed by a question that asked the population the amount of time they have been using a computer. The responses were either 1 year, 5 years, 10 years, or more than 10 years. The population then had the opportunity to determine what they used their computer for most. The possible responses to this question were: research, games, downloading media files, email/instant messaging, data basing and indexing, or an 'other' option (which gave the audience the opportunity to specify their own answer). The population was then asked to choose if they downloaded programs or music daily, weekly, monthly or never. Individuals were then asked to determine if they had come across any computer malfunctions in the past or if they have ever taken a course that may have enhanced their computer knowledge. These questions helped to determine what type of users were being surveyed.

The second goal of the project was to provide information about the toolkit and help determine if the population is aware of it as a security measure. Three questions were produced to retrieve this data. (**Appendix A**) Each question provided an informative paragraph before the question to provide some computer knowledge. The information leading into the first question informed the population of the Sapphire worm and the vulnerabilities of the Microsoft Windows Server 2000 system. The question was made to determine which type of operating systems the population was running. The choices were: Microsoft Windows systems (NT 4.0, 2000. 1998; XP Server 2003; or Millennium Edition (ME)), Macintosh, or an "other" category. The second question gave information about the Microsoft SQL Server Toolkit and how it combats worms and viruses. The third question briefly discussed the Microsoft website and asked the population if they had ever researched the help website or sought help from Microsoft Corporation. Providing information about the toolkit increases public knowledge about security measures that can be taken to combat viruses or worms.

The third goal was to investigate the public awareness of the worms and viruses. The first of these six questions was to determine if the surveyed audience has anti-virus software on their computer and if so, which type. The next questions asked the surveyed population if they were aware of their current network provider's vulnerabilities to infection and if they had some type of warranty or insurance for their hard drive. (**Appendix A**) This segment also had two open-ended questions: one asking the surveyed to comment on any business, personal or social damages they have came across that may be attributed to worms or viruses and the second to comment on what Microsoft's responsibilities should be for its servers. The last question was to determine if the survey had increased their computer knowledge. Individuals were asked to rank the amount of knowledge gained from the survey on a scale of 1 to 10. These questions were constructed to determine the public awareness of worms and virus information.

There are four questions in the survey that provided feedback for goals 2 and 3. The first question was to determine if the users had a Microsoft update informer and how often it updated the software or prompted the user to update software. The second question was to determine if the population had been a victim of a virus or worm infection. The third question asked the target audience if they had come across a computer malfunction they could not completely define. They were to specify what happened and the degree of the malfunction on a scale from 1 to 10. (**Appendix B**) The last question of the survey provided the social implications caused by the Sapphire worm and then asked them to comment if they had or had not been affected by the worm.

3.3 Survey Design Method

There are a few steps that must be followed in order to establish a clear and concise survey. The first step is to establish what the goals of the project are, how they are expected to be reached and what you would like to learn from the survey. Once goals have been set, then the target sample must be determined so you know how will be interviewed. The next procedure is to choose an interview methodology. This is how you will interview the target sample population. After these steps have been accomplished, then it is time to create the questionnaire and pre-test the questionnaire. Once the survey is in final draft form, the next step is to conduct the interview and have the target sample to enter the data. The final procedure is to analyze the data.

3.3.1 Establish Goals

The first step in designing a survey is to determine what one wants to learn and establish clear goals. Establishing the goals will help to determine how, when, and where the survey will be issued. If specific goals are not met, objectives of the survey will not be fully understood and the outcome will not be sufficient enough to prove anything.

The first goal of this project is to figure out which genre of users is filling out the survey and what actions they do that will make them more susceptible. Some of the actions from the questions are downloading frequency and computer usage. This will tell which types of people are affected and what they may have in common. By discovering a common trait among afflicted users, a solution to prevent virus infection can be derived.

The second goal is to discuss the Microsoft toolkit to provide information and increase the knowledge and make respondents aware of the security measure to viruses. We anticipate giving knowledge of the toolkit and worms to people who have been affected and those who have not. The questions that follow this goal are more informative then the rest.

The third goal established was to investigate public awareness of worm and virus information. It is important to know what the users may already know about worms and viruses to determine what they should know or what is missing.

3.3.2 Determine Sample

There are two main mechanisms needed to determine a sample group. The first is to decide on who is to be polled. This group of people is known as the "target market" or "population." The second step is to determine the size of this target. That is, decide how many people are to be surveyed in order to bring back adequate results.

Essentially anyone who used a computer and the Internet was qualified to answer all questions. It is useful to survey other people then WPI students to avoid biased results.

3.3.3 Choosing an Interview Method

This third step is to decide on how one will interview the target population. There are a number of different ways to interview individuals. The types range from personal interviews to mail surveys. The survey method should be based on different elements and logistics. These factors include speed, cost, internet usage, literacy levels, sensitive questions, video, sound and other graphics. Also, it is useful to compare the advantages and disadvantages of each possible data collection method.

One of the methods chosen for this project to use was email surveys. The majority of our target market can be located on the WPI email server. The email survey allows for a quick response from the target population. Aside from speed, another advantage of using an email survey approach is because there is practically no cost involved once it has been completely set up. Email surveys also allow one to add pictures or sound files as attachments. It is also a good choice because the majority of the target population, WPI community and visitors, would respond to an email survey as compared to a phone survey.

The other method that used for data collection is known as scanning questionnaire. During this process, the target population will be provided with printouts of the survey for them to answer. The main advantage of this method is that it provides very accurate information. This allows the project team to get a visual picture of the target population.

3.3.4 Creating the Survey

The next step in achieving useful information through data collection is actually creating the survey. During this phase the project team develops what questions will be asked to the target population.

This project team analyzed the goals in depth to determine which questions would provide adequate feedback. Establishing goals made it easier to develop questions that would provide qualitative data. Throughout this phase, the goal was to design a survey based on the KISS mentality ("Keep It Short and Simple"). In this manner, it was assured that individuals would not be distracted or bored by a long, drawn out questionnaire. A lengthy survey could cause inaccurate or incomplete surveys.

There are three basic types of questions: multiple choices, numeric with open ended, and test open ended. In this survey, all three types of questions were incorporated. There are two types of multiple choice questions: ratings scales and agreement scales. In this survey, the numeric rating scale version was used. The majority of the survey questions required a *yes/no* answer. For each *yes* answer, the individual taking the survey was asked to also elaborate on the answer to further portray information.

3.4 Getting the Survey Out

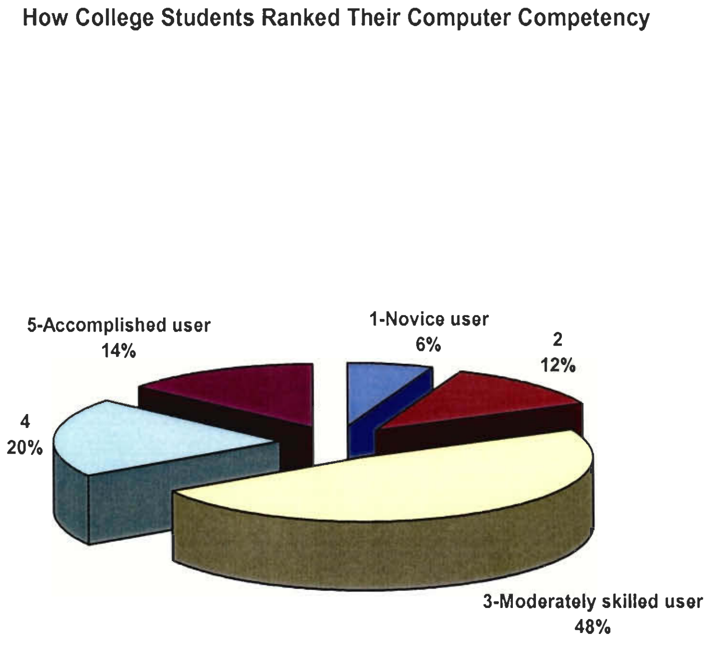
Contacting survey targets was done over a three week period via email, interview, and group distribution. Once completed, participants returned the survey and the results were analyzed for trends. Access to mass email lists for WPI was hard to come by and technical difficulties were encountered in trying to get the survey out to all undergraduates at the school.

Administering the survey proved more difficult than initially anticipated as survey takers often seemed reluctant to complete and return it promptly. As most of the surveys were sent out via email, this created a timeline hurdle. The survey results were vital to attaining the goals. Relying on personal interviews proved difficult as well because people were less likely to answer a question after giving it sufficient thought. A final push to get surveys returned resulted in enough data to base an argument on. In fact, the number of returned surveys used in this investigation was limited to only those completed or having relative information. Many questionnaires came back with extra editorial material from the participant.

4. Survey Results and Analysis

The IQP team determined that college students are the most susceptible group to worm or virus infections based on their high activity of downloading items. This is based on the findings of the survey. These college students typically had been utilizing a computer from 5 to 10 years. This crowd considered themselves as a moderately skilled computer operator ranging from 2 to 4 on a 5 point scale.

Fig. 4.2

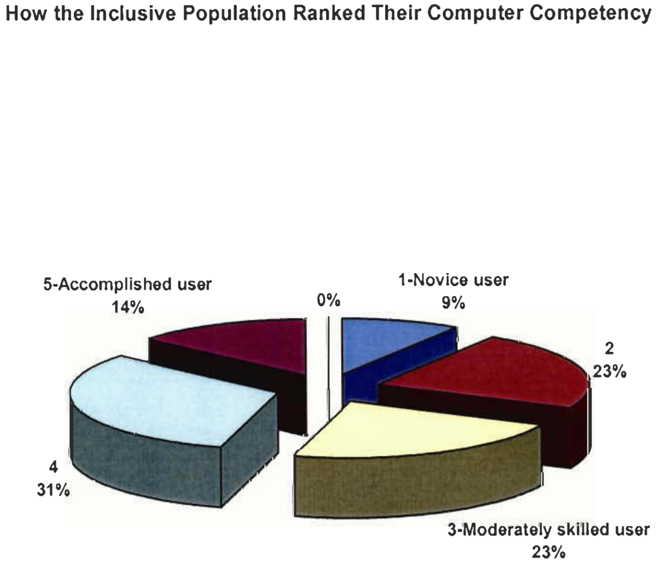


24 of 49 college students ranked themselves a "3" for level of skill use. That's nearly half (48%) of this audience who thought themselves to be moderately adept computer users. Of these 24, nine students said the survey increased their knowledge by ranking a

“6”. Totally, 82% of college students ranked at least a “3” in computer competency. Clearly, college students are more skilled then the rest of the entire survey population.

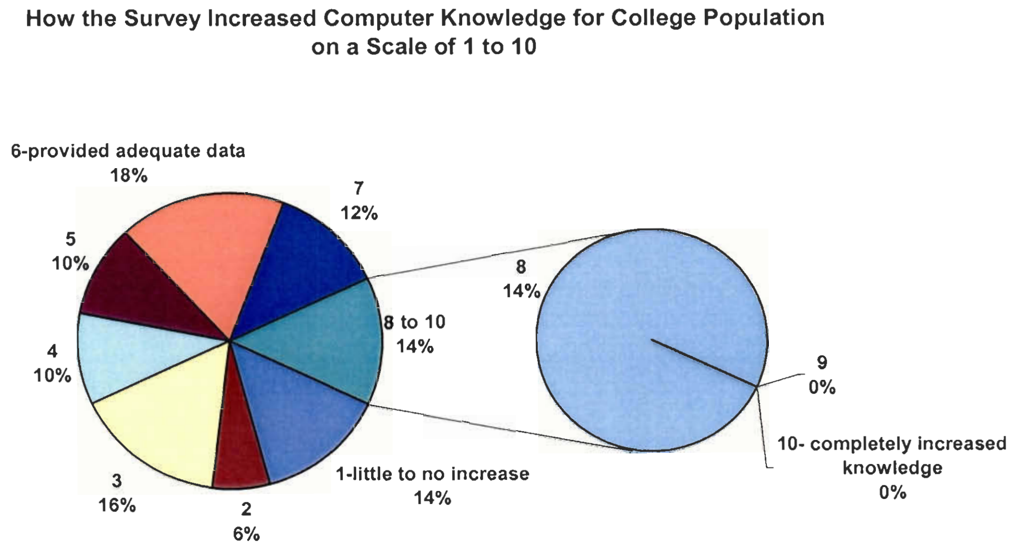
The “other,” or Inclusive Population, category was composed of 22 respondents (all non-college students). Business consultants, laborers, social workers, teachers, and high school students were all included in **Fig. 4.3**. 31% of them rated a “4” on the skill level: the highest percentage of the group. 55% of the total genre viewed themselves at least moderately adept at computer use.

Fig. 4.3



How the Inclusive Population Ranked Their Computer Competency

Fig 4.4



Because of the diversity of professions within this population, scores rating the knowledge gained from the survey ranged fairly distributed from 1 to 7.

Fig 4.5

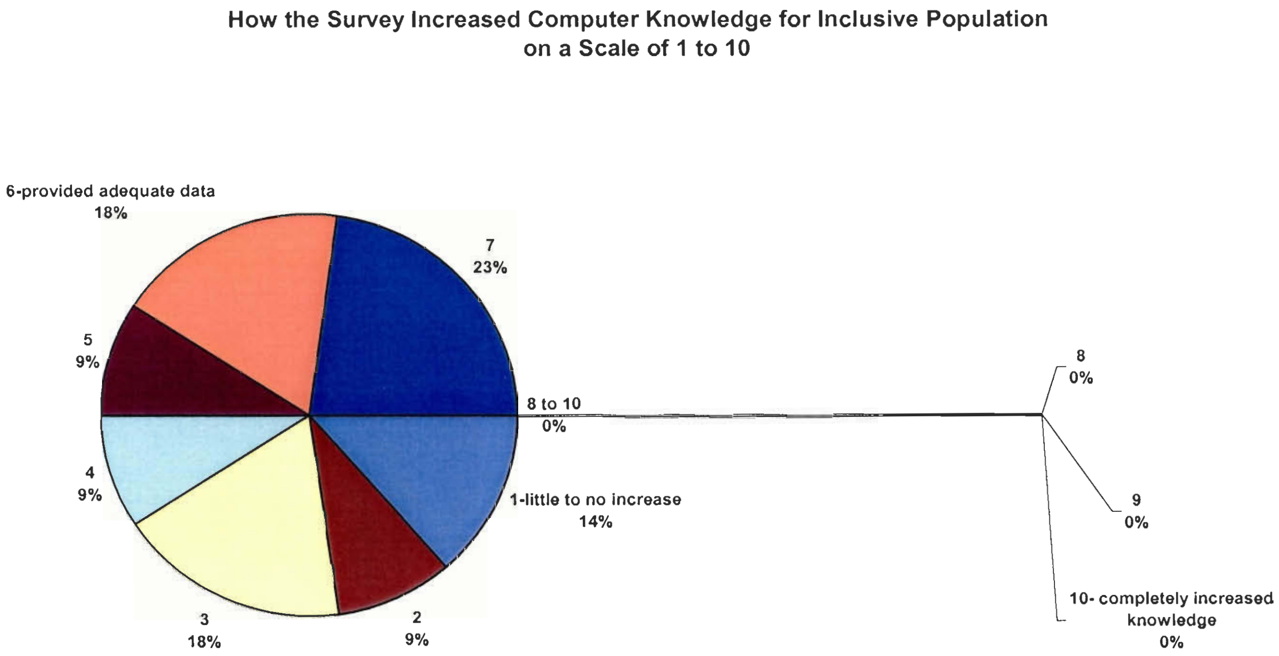
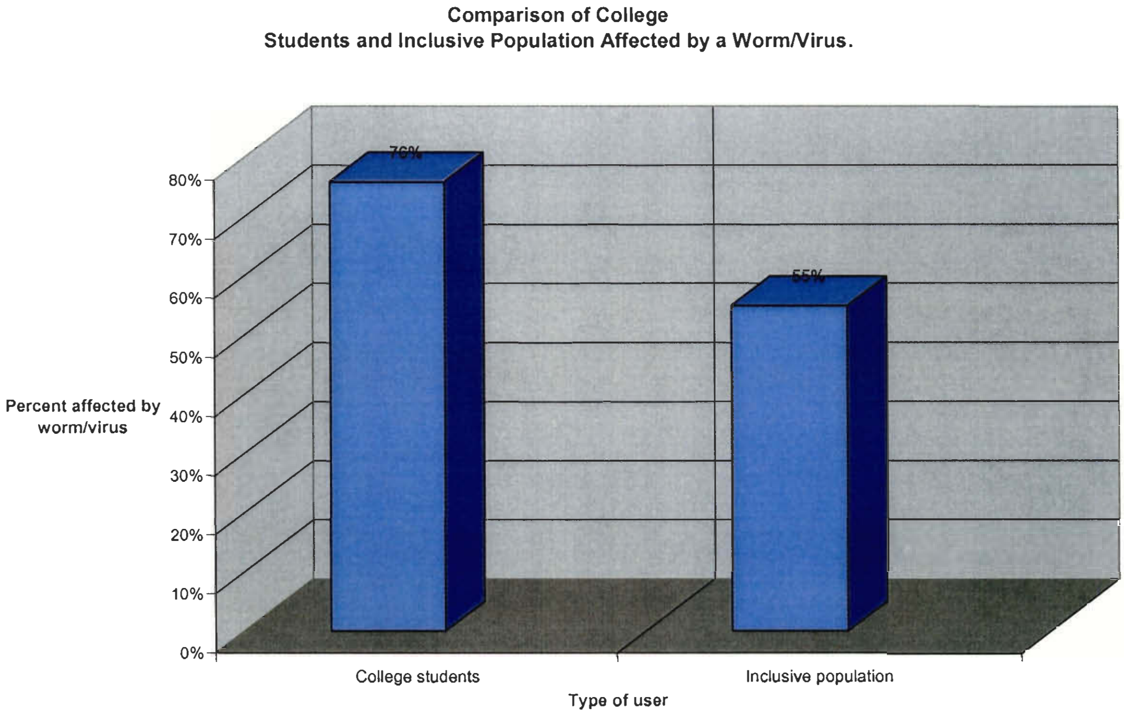


Figure 4.5 is a representation of how the survey increased computer knowledge for the Inclusive Population. Because, of the total group,

Fig 4.6

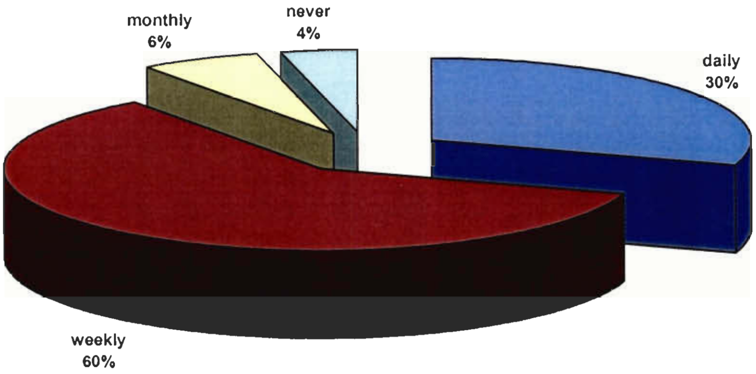


Comparison of College
Students and Inclusive Population Affected by a Worm/Virus.

Despite the fact that college students claim to be more proficient on a computer, a higher percentage of them have been infected by a worm or virus. **Figure 4.6** shows that 20% more of the College Student population has been infected than the Inclusive Population. Totally, 38 college students reported being a victim while only 12 of the Inclusive Population had.

Fig 4.7

How Often College Students Download Media Files, Software Programs, or other Items from the Internet



The majority of this group used their computer for email or instant messaging. **Figure 4.7** shows that they tend to download music or programs daily or weekly. In fact, 90% of the group downloads something from the Internet at least every week (30% daily and 60% weekly)

On the other hand, **Fig. 4.8** shows a more even distribution of how often the Inclusive Population downloads media files, software, etc. It should be noted, however, that there are five people from this group who do not ever download anything. These people are not included in the pie chart.

Fig 4.8

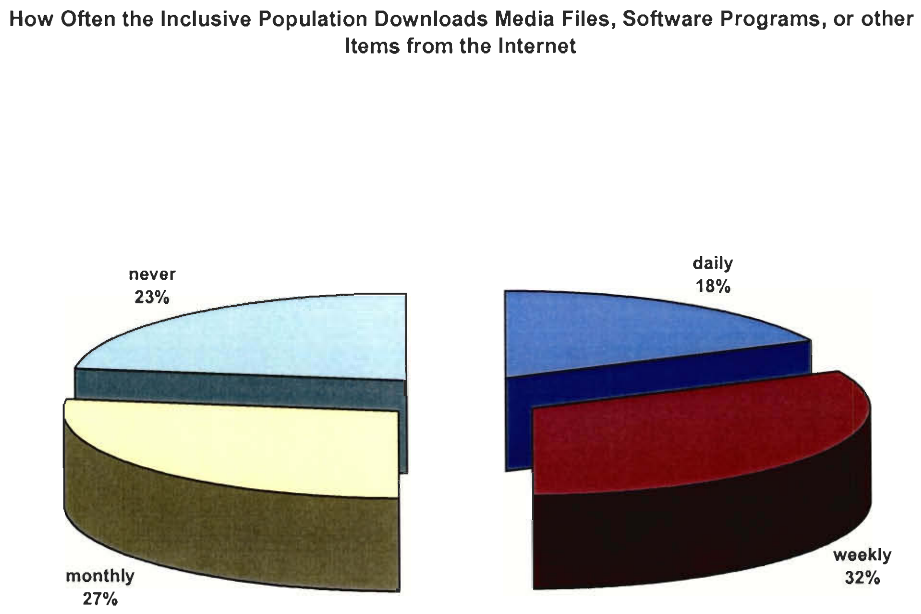
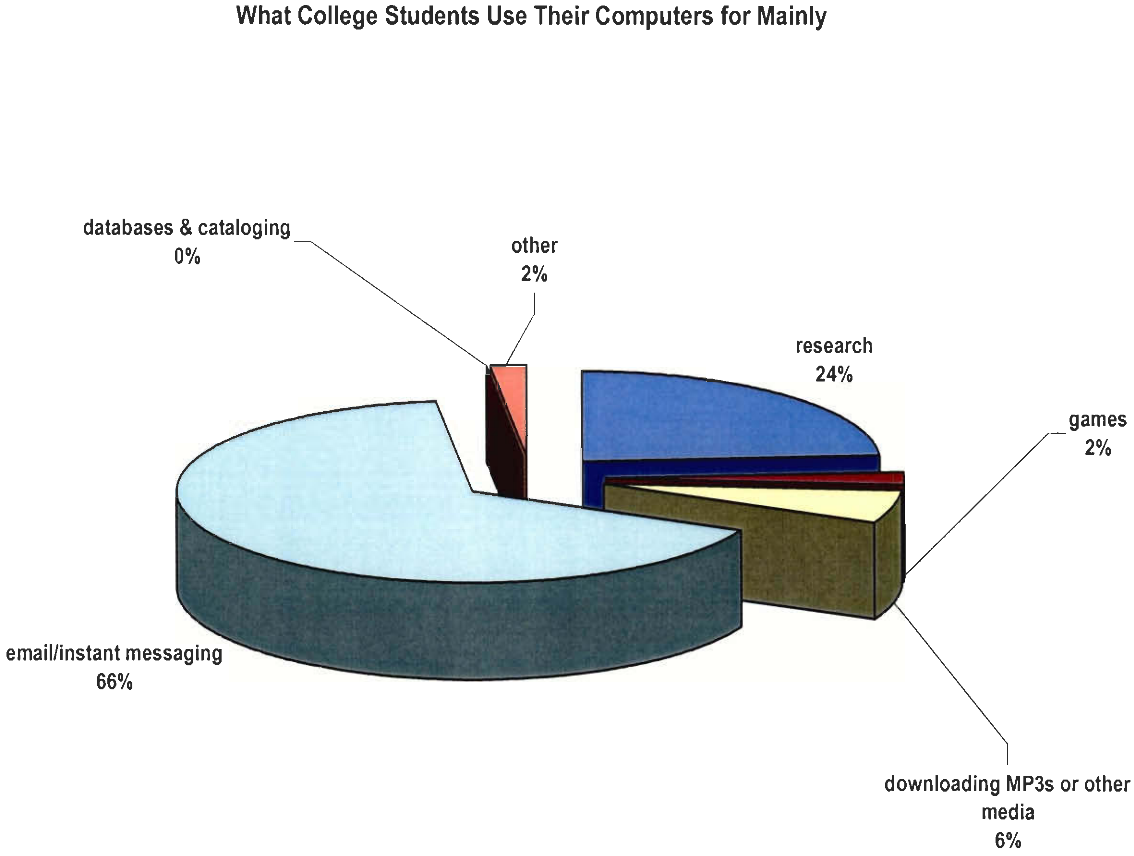
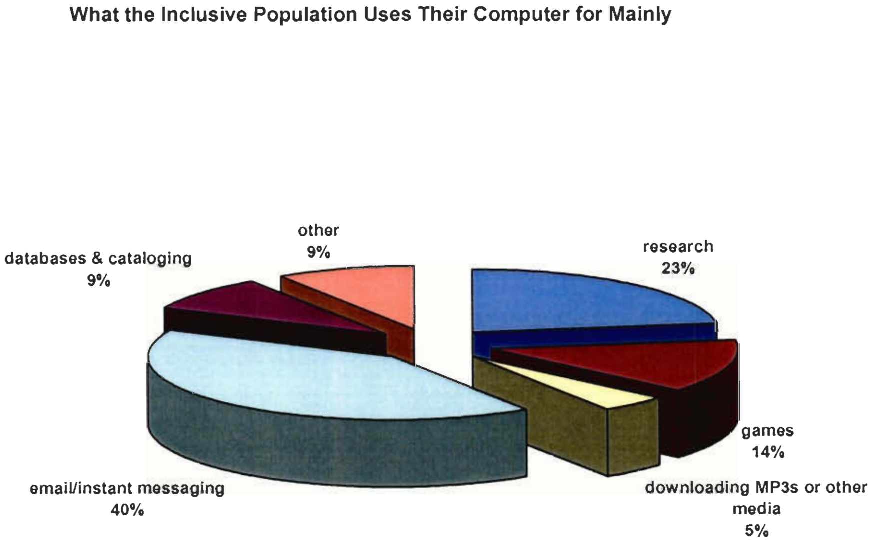


Fig 4.9



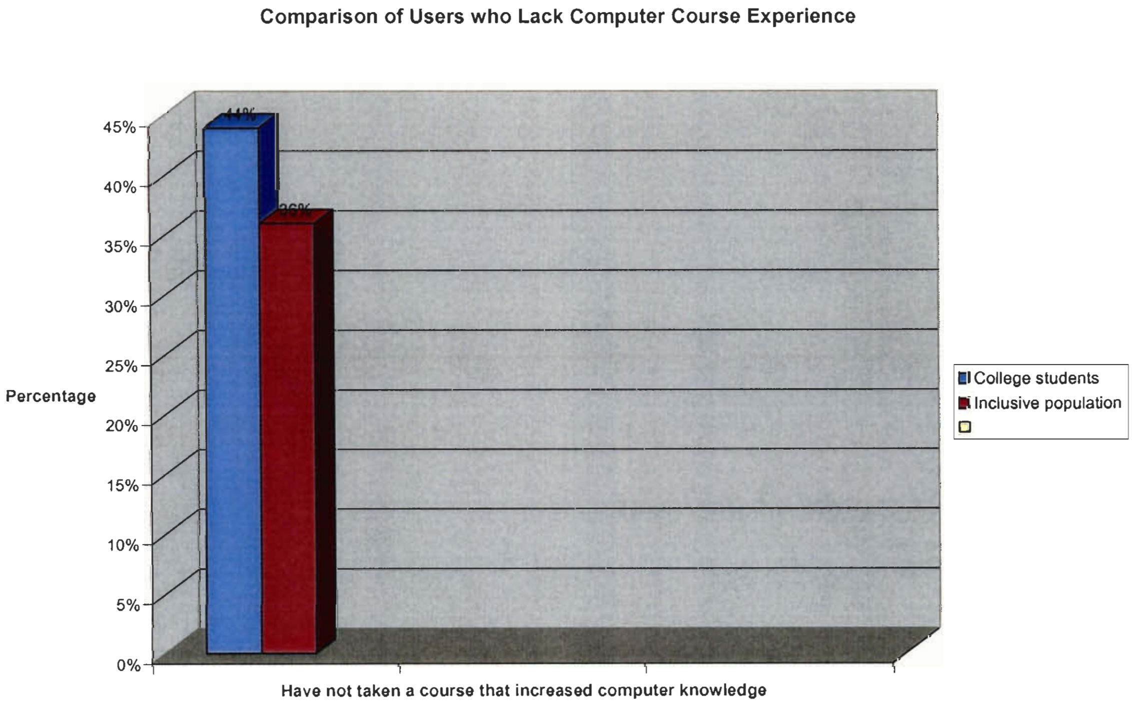
This graph is important to distinguish what actions are taken by the people, or college students, most susceptible to viruses. It is evident that the majority of college students utilize their computer for emailing and instant messaging. Only 34% of the college student population shown in **Fig 4.9** use their computer for other means including games, research, and other actions. This is compared to the 40% of the inclusive population shown in **Fig 4.10** that use the computer for email and instant messaging. It can be noted that college students use email and instant messaging (66%) as much as the inclusive population does not (60%). This supports the argument to determine what individuals are doing on their computer that may distinguish from individuals who are not being affected as much by viruses.

Fig 4.10



It can be expected that all college students take some type of computer course in their college career to enhance their computer knowledge. College students are seen as the new emerging world leaders. Out of the 50 college students surveyed 44% have not taken a computer course. This is 8% more than the inclusive population of people who have not taken a computer course in increase their computer literacy. **Fig 4.11** strengthens the initial hypothesis of a correlation between inexperienced computer users and if they have been affected by a virus. Influencing these numbers is the fact that almost all WPI students have taken a required computer course.

Fig 4.11.



5. Conclusion

5.1 Discussion

Results gained from the survey proved that less experienced users were more readily afflicted by viruses and worms. These users consist of the college student portion of the surveyed population. The compounding of the facts that this group, for the most part, had been using the Internet less, hadn't taken many computer courses, and was often downloading and various files lead to its being the lead victims for virus attack. College students, compared to the rest of the target, received more viruses.

The main findings are based on the comparison and contrast of the college students and inclusive population. One finding is that college students rate their computer literacy higher than others respondents but have been affected by more viruses also. The survey also increased the knowledge of more college students as compared to the inclusive population. Another finding is that college students download programs and files of the Internet more frequently than the inclusive population. The majority of college students use their computer for emailing and instant messaging. The last important finding is that more college students have not taken a computer course as compared to the inclusive population. These findings portray the college student population to be more susceptible to worms as compared to the inclusive population.

5.2 Experimental Errors

Because survey participants were allowed to take the survey at their own discretion, there were often problems with results. For one, many potential results weren't returned in a timely fashion. Or, when a feedback form was returned, a few of them were not in readable format.

Getting the survey out was attempted in the most efficient manner but technical difficulties impeded progress here. A wide network for participants was established through other means and had no affect on final results.

5.3 Summary

The survey design allowed each goal to be directly addressed. The three main goals of this study were 1.) to figure out which genre of users is responding to the survey and their actions performed on a computer, 2.) provide information about the toolkit and inform users it is a security measure to worms, and 3.) investigate public awareness of worm and virus information. Just by volunteering to answer the poll, survey participants were able to advance their comprehension about how viruses and worms work and get beginning insight in how to secure their own PC. A user is more likely to avoid viruses if s/he is well-informed about simple preventative measures.

6. Bibliography

Bourque, Linda Brookover. *How to conduct self-administered and mail surveys*. California: Sage Publications, 1995.

Fink, Arlene. *The survey handbook: Survey kit, vol. 1*. California: Sage Publications, 1995.

Fink, Arlene. *How to analyze survey data*. California: Sage Publications, 1995.

Fink, Arlene. *How to ask survey questions*. London: Sage Publications, 1995.

Fink, Arlene. *How to design surveys*. California: Sage Publications, 1995.

Jolliffe, Flavia R. *Survey design and analysis*. New York: Halsted Press, 1986.

Levy, Paul S. *Sampling of populations: methods and applications*. New York: Wiley, 1999.

Microsoft Corporation. *Finding and fixing Slammer vulnerabilities*. 2003. Internet on-line. < http://www.microsoft.com/security/slammer.asp> [February 2004]

Microsoft Corporation. *SQL Server 2000 Security Tools*. 2003. Internet on-line. <http://www.microsoft.com/sql/downloads/securitytools.asp> [February 2004]

Microsoft Corporation. *What you should know about the Blaster Worm and its variants*. 2003. Internet on-line. < http://www.microsoft.com/security/incident/blast.asp> [February 2004]

Poulsen, Kevin. *Slammer worm crashed Ohio nuke plant network*. Internet on-line. Available from http://www.securityfocus.com/news/6767. [August 2003]

Symantec. *W32.Blaster.Worm Removal Tool*. 2003. Internet on-line. <http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.removal.tool.html> [March 2004]

Appendix A.

Please select the *single best possible* selection for each of the following questions:

Q-1 Please choose a category that describes you:

[ ] *WPI Student*
[ ] *WPI Faculty*
[ ] *WPI Staff*
[ ] *Business consultant*
[ ] *High school student*
[ ] *Other (please specify)*

Q-2 How would you rate your ability to operate a computer? (1-5)

(1-novice, 3- moderately skilled, 5-accomplished)

1 2 3 4 5

Q-3 How long have you been using a computer and the Internet on a regular basis?

[ ] *1 year*
[ ] *5 years*
[ ] *10 years*
[ ] *10+ years*

Q-4 What do you use your computer for the most?

[ ] *Research*
[ ] *Games*
[ ] *Downloading MP3s or other media*
[ ] *Email/Instant Messaging*
[ ] *Databases and cataloging*
[ ] *Other (please specify)*

Q-5 How often do you *download* music, programs, or other information from the internet?

[ ] *Daily*
[ ] *Weekly*
[ ] *Monthly*
[ ] *Never*

Q-6 If you have had computer malfunctions in the past, how did you resolve them?

(Did you fix the problem or seek outside help? Specify.)

[ ] *Yes…*

[ ] *I have not, to my knowledge, encountered computer malfunctions.*

Q-7 Have you ever taken a course that increased your computer knowledge?

[ ] *Yes*

If yes, specify what material was taught and what you recall.

[ ] *No*

The Slammer/Sapphire/Blaster Worm affects three vulnerabilities in the Microsoft Windows Server 2000 system. The worm operates through a process called random scanning. It randomly selects vulnerable IP addresses until a susceptible host is found and then replicates itself by to that address. Because it seeks data in a random faction, it is highly efficient in replicating itself from computer to computer.

Q-8 What operating system are you running?

[ ] *Microsoft Windows NT 4.0*
[ ] *Microsoft Windows 2000, 1998 or other*
[ ] *Microsoft Windows XP*
[ ] *Microsoft Windows Server 2003*
[ ] *Microsoft Windows ME*
[ ] *A form of Macintosh*
[ ] *Other (please specify)* ________________________________

The Microsoft SQL Server Toolkit terminates the Slammer/Sapphire/Blaster Worm, deletes the worm files, deletes the dropped files and deletes the registry values that have been added by the worm. The toolkit completes this process through three stages: SQL Scan, SQL Check, and SQL Critical Update.

Q-9 Are you aware of the Microsoft SQL Server Toolkit as a remedy?

[ ] *Yes*
[ ] *No*

Microsoft.com provides useful information for users looking to resolve computer vulnerabilities. The website provides a history of information for every worm/virus that Microsoft has come across. The website also contains a customer service portion for quick and efficient help.

Q-10 Have you ever had to research or interact with Microsoft Corporation to fix a bug or infection on your hard drive? How reasonable and helpful were the contacts you established? Please elaborate…

[ ] *Yes,*

[ ] *No*

Over the past few years, free anti-virus software has been made available online and most new computers come installed with some form of anti-virus software.

Q-11 Does your PC currently have up to date anti-virus software?

[ ] *MacAfee*
[ ] *Norton*
[ ] *AVG*
[ ] *Other (please specify)* ________________________________
[ ] *I'm not sure what the software is or I'm not sure if my computer has such software*
[ ] *My computer does not have anti-virus software.*

Q-12 Do you know about your current network's (internet provider's) vulnerabilities to worm infection?
[ ] *Yes*
[ ] *No*

Q-13 Do you have a warranty or other form of insurance on your hard drive that covers worm or virus infections?
[ ] *Yes (What does the warranty cover and at what cost?)*

[ ] *No*

Q-14 What business, personal, security or other social damages, if any, have affected you personally and can be linked to computer worms or viruses?

Q-15 On a scale of 1 to 10, has this survey increased your computer knowledge? (1-no increase, 10-great increase)

1 2 3 4 5 6 7 8 9 10

Q-16 To what degree do you think Microsoft should extend its responsibilities in caring for its servers? Should it be concerned with "patching" vulnerabilities or with limiting possible damages caused by an infection? To what extent is it the consumer's dependability to protect a network or PC?

To decrease computer malfunctions, Microsoft has provided an update function on the majority of their computer operating systems. The update function alerts users when Microsoft has developed new software. In most cases, the update alert occurs when the operator turns on their computer.

Q-17 Does your computer have a Microsoft update informer?

[ ] *Yes (if yes, do you take heed to the alerts?)*

[ ] *yes* **If yes, how often does it give you the option to update your software?**

[ ] *every 7 days*
[ ] *every month*
[ ] *every 3 months*
[ ] *every 6 months*
[ ] *longer than 6 months*

[ ] *no*

[ ] *No*

Q-18 Have you ever been a victim of a virus or worm infection?

[ ] *Yes*

If yes, what is the name of the virus or worm?

[ ] *No*

Q-19 Have you ever come across a computer malfunction that you could not define?

[ ] *Yes*
[ ] *No*

If yes, please describe.

Q-20 Have you ever contracted a virus?

[ ] *Yes*

If yes what was the name of the virus?

[ ] *No*

Q-21 How did the virus affect you? Could you determine what was wrong with your computer? What was damaged and to what extent (on a scale of 1 to 10, 1 being slight damage)**?**

1 2 3 4 5 6 7 8 9 10

The Slammer/Sapphire worm began to slow down the internet on January 25, 2003. The worm doubled in size every 8.5 seconds. More than 90% of vulnerable hosts were affected in 10 minutes. It caused numerous social implications including canceled air flights, ATM failures (Bank of America), and election interference.

Q-22 Were you affected by this worm?

[ ] *Yes*
[ ] *No*

If yes, explain.

APPENDIX B.

Q-1	Q-2	Q-3	Q-4	Q-5	Q-6	Q-7	Q-8	Q-9	Q-10
student	4	10+	research	weekly	yes	yes	XP	no	no
other	5	10+	email/IM	monthly	yes	yes	XP	no	no
student	3	5	email/IM	weekly	yes	yes	XP	no	no
high school	4	10	email/IM	daily	yes	yes	2000, 1998 or other	no	no
faculty	4	10	email/IM	weekly	yes	yes	2000, 1998 or other	no	no
other	3	5	email/IM	weekly	yes	yes	2000, 1998 or other	no	yes
student	3	5	email/IM	daily	yes	yes	XP	no	no
student	5	10	email/IM	weekly	yes	yes	other	yes	no
student	4	5	research	monthly	yes	yes	XP	no	no
other	2	10	research	daily	yes	no	XP	no	no
student	2	5	research	weekly	yes	yes	XP	no	no
student	3	5	email/IM	weekly	yes	yes	XP	no	no
business co	5	10+	research	weekly	yes	yes	XP	yes	yes
student	4	5	downloading M	weekly	no	no	XP	yes	no
student	1	5	games	weekly	yes	no	XP	no	no
student	5	10+	email/IM	daily	yes	no	XP	no	no
other	3	5	email/IM	daily	yes	no	XP	no	no
student	5	10	email/IM	weekly	yes	no	XP	no	no
student	3	5	email/IM	weekly	no	yes	XP	no	no
student	3	5	research	weekly	yes	yes	XP	no	no
student	1	5	email/IM	daily	yes	no	2000, 1998 or other	no	no
other	1	5	downloading M	daily	no	no	a form of Macintosh	no	no
student	4	5	research	weekly	yes	no	XP	no	no
faculty	5	10+	other	weekly	yes	yes	XP	no	no
student	3	10+	other	monthly	yes	yes	XP	no	no
student	3	5	email/IM	weekly	no	no	XP	no	no
student	5	10	research	daily	yes	no	XP	no	yes
student	3	10	email/IM	monthly	yes	yes	XP	no	no
other	4	5	downloading M	weekly	no	yes	XP	no	no
faculty	3	10	email/IM	weekly	yes	yes	XP	no	no
student	3	5	email/IM	daily	yes	yes	XP	no	no
student	3	5	email/IM	weekly	yes	yes	XP	yes	yes
student	4	5	email/IM	daily	yes	yes	XP	yes	no
student	5	10+	email/IM	daily	yes	yes	XP	yes	yes
high school	2	5	games	never	no	no	2000, 1998 or other	no	no

other	2	1	games	never	no	no	2000, 1998 or other	no	no
student	4	5	research	daily	yes	yes	XP	no	no
student	3	5	email/IM	daily	yes	yes	XP	no	no
student	3	5	downloading M	daily	no	yes	XP	no	no
student	3	5	email/IM	weekly	yes	no	XP	no	no
student	3	10	email/IM	weekly	no	no	XP	no	no
other	1	5	research	never	yes	yes	2000, 1998 or other	no	no
student	4	5	email/IM	weekly	no	no	XP	no	no
student	4	5	email/IM	weekly	no	no	XP	no	no
student	4	5	email/IM	daily	no	no	XP	no	no
other	2	5	games	weekly	yes	yes	XP	no	no
business co	5	10+	email/IM	daily	yes	yes	XP	yes	yes
student	3	5	email/IM	weekly	yes	yes	XP	yes	yes
student	3	10	email/IM	weekly		no	XP	yes	no
student	2	5	email/IM	weekly	yes	yes	XP	no	no
student	2	5	email/IM	weekly	yes	no	XP	no	no
student	3	5	email/IM	weekly	yes	yes	XP	no	no
student	3	5	research	daily	yes	no	XP	no	no
student	5	10+	research	daily	yes	no	other	no	yes
other	4	10+	research	weekly	yes	yes	2000, 1998 or other	no	yes
other	2	5	email/IM	never	yes	no	XP	no	no
other	2	5	email/IM	never	yes	yes	XP	no	no
other	3	5	email/IM	weekly	yes	yes	2000, 1998 or other	no	yes
other	3	10+	databases and	never	yes	no	NT 4.0	no	no
other	3	5	research	monthly	yes	yes	2000, 1998 or other	no	no
other	3	10	research	monthly	yes	yes	2000, 1998 or other	no	no
business co	3	10	email/IM	monthly	yes	no	2000, 1998 or other	no	yes
other	3	5	email/IM	never	yes	yes	XP	no	no
high school	4	10	email/IM	weekly	yes	no	XP	no	yes
other	1	1	other	never	no	no	2000, 1998 or other	no	no
business co	2	10	databases and	monthly	no	yes	XP	no	no
other	2	5	email/IM	weekly	yes	no	XP	no	no
other	4	10	email/IM	monthly	yes	yes	XP	yes	no
other	4	10+	research	monthly	yes	no	XP	no	yes
other	4	10	research	weekly	yes	yes	2000, 1998 or other	no	no
other	3	5	email/IM	daily	yes	yes	XP	no	no
student	3	5	email/IM	weekly	yes	yes	XP	no	no

Q-11	Q-12	Q-13	Q-14	Q-15	Q-16	Q-17a	Q-17b	Q-18	Q-19	Q-20	Q-21	Q-22
Norton	yes	no		5		yes	every 7 days	no	no	no		no
Norton	yes	no		2		yes	every 3 months	yes	yes	no		yes
Norton	no	no		7		yes	every 7 days	yes	yes	yes	4	yes
Norton	no	no	NA	3	x	no		no	no	no		no
MacAfee	no	no		1		no		no	yes	yes		no
norton	no	yes		6	wise	yes	no	yes	no	yes	9	yes
MacAfee	yes	no	NA	5	wise	yes	every month	yes	no	yes	1	no
Norton	no	no		1		yes	every 7 days	yes	no	no		yes
MacAfee	no	no	NA	4	x	yes	every 7 days	yes	no	no		no
Norton	no	no		7		yes	every month	yes	yes	yes	2	yes
I'm not sur	no	no		6		yes	every 7 days	yes	yes	yes	3	yes
Norton	no	no	X	8	consume	yes	every 7 days	yes	no	yes	4	yes
macafee	yes	yes		3		yes	every 7 days	yes	yes	yes	1	yes
Norton	yes	no	NA	3	x	yes	every 7 days	no	no	no		no
Norton	no	no		6		yes	every month	yes	yes	yes	3	yes
My comput	yes	no	x	1	x	yes	every month	yes	no	yes	4	no
Norton	no	no		3		yes	every 7 days	no	no	no		no
MacAfee	no	no		3		yes	every month	yes	no	yes	7	yes
MacAfee	no	yes		5		yes	every 7 days	no	yes	no	5	no
macafee	no	no		6		yes	every 7 days	yes	yes	yes	6	yes
I'm not sur	no	no		8		no		yes	yes	yes	3	yes
Norton	no	no		7		no		no	no	no	1	yes
Norton	yes	yes		2		yes	every 7 days	yes	no	yes	7	no
Norton	no	no	NA	6		yes	every 7 days	no	no	no	NA	
I'm not sur	no	no	x	3	x	yes	don’t know	yes	yes	yes	10	yes
Norton	no	no		1		no		no	no	no	1	no
MacAfee	yes	no	x	1		yes	every month	yes	yes	yes	3	no
MacAfee	no	no		2		yes	every 7 days	yes	yes	yes	8	no
Norton	no	yes		7		yes	every month	no	yes	no	3	yes
Norton	no	no		2		yes	every 7 days	no	no	no		no
MacAfee	yes	no	NA	5	wise	yes	every month	yes	no	yes	1	no
macafee	no	no		4		no		no	no	no	5	no
MacAfee	no	no		6	wise	yes	every 7 days	yes	no	yes	3	no
macafee	yes	yes		3		yes	every 7 days	yes	yes	yes	6	yes
macafee	no	no	NA	6	X	no		yes	yes	yes	9	no

I'm not sur	no	no	NA	7		no		no	yes	no		no
Norton	no	no		6		yes	every 7 days	yes	yes	yes	3	no
Norton	no	no		7		yes	every month	yes	yes	yes	2	yes
Norton	no	no		8		yes	every month	no	yes	no		no
MacAfee	yes	yes		3		yes		no	no	no		no
Norton	no	no	NA	1	X	yes	every 7 days	yes	no	yes	1	no
I'm not sur	no	no		3				no	no	no		no
Norton	yes	no	NA	6		yes	every month	yes	no	no		no
Norton	yes	no	NA	1	x	yes	every month	yes	no	no		no
MacAfee	yes	no	NA	4		yes	every month	no	no	no		no
macafee	no	no	n	8		yes	every month	yes	yes	yes	4	no
macafee	yes	yes		3		yes	every 7 days	yes	yes	yes	3	yes
Norton	no	no		7		yes	every 7 days	yes	yes	yes	7	yes
My comput	no	no	NA	4	x	yes	every month	no	no	no		no
none	no	no				yes	every 7 days	yes	yes	yes		yes
Norton	no	yes		4		yes	every month	yes	yes	yes	4	no
Norton	no	no	NA	3	x	yes	every month	yes	yes	yes	10	no
MacAfee	no	no		7		yes	every month	yes	no	no	2	no
Norton	no	no		1		no		no	no	no		no
MacAfee	no	no		8	x	yes	every 7 days	yes	no	yes	10	no
Norton	no	no		6		yes	every month	yes	yes	yes	10	no
Norton	no	no		5		no		no	no	yes		
Norton	no	yes		6		yes	no	yes	no	yes	9	yes
MacAfee	no	no		6		yes		yes	no	yes	8	no
MacAfee	no	no	na	5		no		yes	yes	yes	6	no
MacAfee	no	no		8		yes	every month	yes	yes	yes	1	no
other	no	no		1		yes	every 7 days	yes	no	yes	8	no
MacAfee	no	no		2		yes	every 6 months	yes	no	yes	2	no
MacAfee	no	no	na	6		yes	every 7 days	yes	no	yes	6	no
I'm not sur	no	no		4		no		no	no	no		no
MacAfee	yes	yes	na	4		yes	every month	no	yes	yes	3	yes
My comput	no	no	na	5		yes	every month	yes	yes	yes	10	no
MacAfee	yes	no		3		yes	every 7 days	yes	no	yes	8	no
MacAfee	yes	no		1		yes	every 7 days	yes	yes	yes		no
MacAfee	no	no		7	x	no		yes	yes	yes	1	no
norton	no	no		7		yes	every 7 days	yes	no	yes	6	no
Norton	no	no		7		yes	every month	yes	no	yes	1	no