Salisbury
UNIVERSITY

Honors College

Honors Thesis

An Honors Thesis Titled

Human Catalysts: Behavior Causing the Spread of Computer Viruses

Submitted in partial fulfillment of the requirements for the Honors Designation to the

Honors College

of

Salisbury University

in the Major Department of

Mathematics and Computer Science

by

Kayla Cannon

Date and Place of Oral Presentation: SUSRC - April 2017

Signatures of Honors Thesis Committee

Mentor:		Dr. Randall Cone
Reader 1:		Dr. Donald Spickler
Reader 2:		Dr. Betty Lou Smith
Director:		James J. Buss
	Signature	Print

Abstract

This study focuses on highlighting the importance of personal protection from computer viruses. This issue is approached by way of releasing a survey, which is intended to investigate our main question of "How well does the public understand about their role in the control and spread of computer viruses?" We challenge the idea that all users are responsible enough to safely operate a computer system. Data collected at the end of the survey is analyzed, manipulated by data filters which output a selection of survey responses based upon given criteria. Statistics are calculated based on the output from the data filters. To ensure the anonymity of each respondent, the survey does not ask questions that reveal any personal information. A behavioral analysis is completed to investigate safe behaviors people should use while operating a computer. Overall, this investigation is meant to stimulate a spread of education about computer viruses.

Introduction

"A virus is a computer program that hides inside another program . . . that attempts to propagate itself to other computers, and that often includes some destructive function" (Salomon 37). Viruses have become more prevalent over recent years due to our ever-growing dependence upon computers. In today's world, individuals and corporations alike rely on the functionality of computers to send and receive data and this transmission increases the likelihood of being infected with a computer virus. This fact alone serves as a reminder that all computer users should be more aware of how their actions help spread harmful viruses.

In this paper, we investigate the level of understanding the public has about protecting themselves against computer viruses and promote virus protection. This issue is approached by way of releasing a survey, which asks respondents questions about the unsafe behaviors they practice while operating either a personal or public computer. Such behaviors are analyzed to find a correlation between those currently using unsafe behaviors and those who claim to bring about behavior change.

To develop a plan to further educate the public on safety guidelines, we should first consider educating the public on what exactly computer viruses are. Users need to know the dangers of viruses before they can be taught how to avoid such malicious software in the future. Examining multiple types of computer viruses as well as their abilities gives users valuable information that allows them to develop more cautious behaviors. A virus's ability is considered here to be how the virus infects the host computer as well as how the virus spreads from host to host.

Virus Definition

A computer virus is malicious software that "resides in an executable file and propagates to other executables" (Salomon 37). Whenever the host executes instructions, the virus within said host also executes certain instructions (Salomon 41). A virus may contain certain instructions which, when run, will make the virus "spread through the infected machine or across to other machines" (Buckland 88). While many viruses cause "untold damage" (Buckland 91) some are designed to be benign, mostly as a distraction or annoyance to the user (Buckland 88). What categorizes a virus as benign is the characteristic of not directly causing harm to the host computer.

Virus Propagation

Viruses contain instructions that tell the software how to propagate, that is, move from computer to computer, and inflict damage. Depending on the intentions of the virus creator, a virus can spread itself throughout its host in a multitude of ways. For example, a computer virus can spread once it is attached to either a file or an executable program. If a virus infects a given program, the virus "is executed every time the program is executed" (Salomon 49). In contrast, if a virus infects a file, it can only spread once the infected file is transferred to or accessed by other systems. When an infected file is emailed to and opened by a user, the embedded virus executes (Salomon 49). Infected files can also penetrate a host if the user downloads "files from the internet" (Singhal 30). Another way that viruses are spread is through the sharing of external data drives. The risk of infection exists whenever "users share a computing resource such as a disk" (Salomon 50). If an infected drive is accessed by a computer, any malicious software present will be transferred, and consequently infects the host machine. Studies have shown that using "removable storage media" can increase the rate in which viruses are spread (Zhang 420).

The Home User

When it comes to personal protection, "[t]he home computer user is often said to be the weakest link" (Howe et al., 209). Home users are not necessarily computer professionals: although they use them for many facets in their lives, they do not undergo training on how to use their computer (Howe et al., 209). Because of this, "computer users often do not adequately understand" the many threats faced by their system and do

not always have the "knowledge to be able to handle them" (Howe et al., 209). Personal security can be improved once a better connection is made between software developers and users. Developers should "better understand what influences decisions about security for the home computer user" and only then can we implement better security measures (Howe et al., 209).

While operating a computer, users make security decisions despite their knowledge level on the topic (Wash and Rader 1). To properly make these decisions, users need to have extensive "knowledge about computers and computer security issues" (Wash and Rader 2). It has been found that users having "more knowledge about common security issues [are] frequently found to . . . behave securely" (qtd. in Wash and Rader 2). It becomes problematic for users to make such important decisions when they "rarely know for sure if they are making the 'correct' ones" (Wash and Rader 11). When speaking on teaching users how to effectively protect themselves from viruses, "[m]ost people struggle to learn . . . how to protect themselves from computer security threats" (qtd. in Wash and Rader 11).

A study conducted by Rick Wash and Emilee Rader resulted in the formulation of common beliefs users have about computer viruses. Two of these include the idea that viruses are contracted over the internet and cause visibly noticeable problems for the host computer (Wash and Rader 5). The third and most important belief is that users can protect themselves from such software (Wash and Rader 5). Users also understand that taking part in behaviors such as "[c]licking on advertisements, downloading files . . . or simply visiting the wrong webpages" can lead to an infection, especially when not using "an anti-virus software to scan downloads" and other files on the host machine (Wash

and Rader 5). If they do not already, users should use cautious behaviors while operating their computers, such as creating strong passwords for online accounts, backing up data regularly, and using antivirus software and firewalls (Ng et al., 816).

Personal Protection

One major problem with users protecting themselves from computer viruses is knowledge of the behaviors of other users. Those who are ignorant of personal security strategies are those who put their system and others at risk. Not all users know how to effectively protect themselves from infection and tend to "look for shortcuts and workarounds, especially when users do not understand why their behavior compromises security" (qtd. in Pfleeger and Caputo 599). Shortcutting security systems, whether accidental or purposely, compromises all information on the computer. Apart from shortcutting security, uneducated users "may be overwhelmed by difficulties in security implementation, or may mistrust, misinterpret or override the security" (Pfleeger and Caputo 598). Users who do not understand or work around security measures are not capable of protecting themselves and others from infection.

Because computer viruses still exist, it is obvious that there are users who do not protect themselves from infection either purposely or ignorantly. For those who are ignorant but eager to learn about cyber security and virus protection, there should be a way to get them to understand the significance of personal protection. Since personal security is not a "primary task" of users using technology today, "system developers often focus on these primary tasks before incorporating security into an architecture or design" (Pfleeger and Caputo 600). Developers are creating software that does not

explicitly protect users from outside threats. Therefore, when users are executing said software, they can be put at risk because of a mistake or risk made by the developers. Not only does this put the user at risk of possible infection, but blames said infection on the user. In other words, people who unknowingly use unsecure software are creating a stereotype of a careless user, while the blame should be on the developers for creating software that puts its users at risk.

When software developers do in fact put safety measures in place in their software, they are too complicated and aggravating for the user to effectively implement. When people sense they are being forced to complete a certain task, it is less likely the task will be done. In this case, the more users who feel forced to work under safety precautions, the more likely they are to have risky behaviors. In an examination where users were forced to change their account passwords, "the changes were intentionally delayed and the request perceived as being an unnecessary interruption" (qtd. in Pfleeger and Caputo 598). For many online services, changing the password for a personal account is an easy step to take to ensure personal security. However, many users are reluctant to take this step because they do not find security important and the change is perceived as more of a burden than a benefit.

Frequent password changes can be frustrating for users. Not only are you recommended to change said password, but you also must somehow store these new passwords for later use. For users with multiple online accounts, each with their own unique password, there exists the problem of remembering and safely storing these passwords.

While operating a computer, the user is responsible for implementing precautionary behaviors to maintain the system's security. Many of these precautions are easy for a user of any skill level. It is suggested for each user to employ these tactics as often as possible:

(1) Use caution when installing programs from the internet. You should "[a]lways research any programs you wish to install" (Singhal 30).

(2) Avoid 'bad' websites at all times. These websites are adult or piracy sites or any other sites that involve sharing files (Singhal 30).

(3) Do not open emails from unknown senders and especially do not click on any links embedded in said emails (Singhal 30).

(4) Regularly update your operating system. This blocks any holes in security that can be used as pathways to infect the system (Singhal 30).

(5) Regularly update your antivirus software. Making sure the program is updated ensures that you will get the best protection against newly found viruses (Singhal 30).

Virus Detection

There are warning signs to look for if a computer is believed to be infected with a virus. Common symptoms of a computer virus include "[sudden] poor performance" (Spector 28) along with "[s]tandard maintenance programs" not working properly, and

"[y]our home and search pages [changing]" (Spector 29). Based on these symptoms, you should be suspicious when "your PC is running slower than it used to" or when "programs . . . fail to work" and if your home page "[changes] to something you don't want" (Spector 29). Other symptoms include having multiple windows randomly appear on the monitor, discovering small data files in the hard drive, as well as losing important data (Singhal 30). An infected computer may also begin to "[crash] more frequently or sometimes . . . shutdown automatically" (qtd. in Singhal 30).

Antivirus Software

Multiple brands of anti-virus software implement what is known as a dynamic heuristic scanning technique, which scans the host computer for any malicious activity. Scanning the host system in this manner is meant to "closely monitor the operating system (OS) and preserve the normal operation of the system" (Bo et al., 20). The technique intercepts "malicious and illegal procedures" (Bo et al., 20). For this technique to work, however, the phrase 'illegal procedure' must be defined so they can be found on a system. An illegal virus is characterized by the following:

(1) "[Modifying] the total system memory to remain concealed from the disk operating system" (Bo et al., 20).

(2) Causing the "antivirus system [to execute] commands before the host program" (Bo et al., 20).

The dynamic heuristic scanning technique executes four main tasks within antivirus software. These tasks include "detecting "the user's network connection" and "[ensuring] the safety of users whose internet usage is within a certain range", [sending] a warning to

network users" while "[determining] the internal behavior of unauthorized networks", as well as "[determining] the potential danger program" (Bo et al., 20).

Viruses Infecting Companies

Small companies and large corporations are also at risk of virus infection because "hackers are using viruses with increasing frequency. . . which extorts a ransom from companies to regain access to their own data" (Mahoney, 2016). It is recommended that companies should "hire an outside company to do penetration testing and try to hack into their systems. . . to see where they are most vulnerable" (Mahoney, 2016). Another plan to improve the company's protection involves the knowledge of its employees. The education of all employees "is vital" and "training should be mandatory to help employees identify different types of cyber attacks that could occur to the company system" (Mahoney, 2016).

Viruses and Risk Perception

Users can be partially blamed for the continuation of cyber attacks because of the risk they perceive of being a target of such an event. When small companies are specifically targeted, the resulting infections can be traced to employees. To reduce the risk of a company's systems being infiltrated, the following three issues must be considered, including the "employees' beliefs about probabilities and consequences of a virus attack", along with each employee's "self-perception of being competent with Information Technology" and analyzing "the daily behavior of employees" (Mariani and Zappalà 52). Employees are more likely to cause a company-wide virus outbreak if they partake in unsafe behaviors and if they believe their chance of infection is low.

When analyzing preventive behavior, two models, the Precaution Adoption Process Model and the Health Belief Model, are useful. The Precaution Adoption Process Model considers a sequence of steps that must be taken to prevent a certain behavior. First, "individuals have to realize that a specific risk exists". Second, it must be realized "that the risk is significant and can affect them and/or other people". Third, "they have to realize that they are vulnerable to the risk" (qtd. in Mariani and Zappalà 54). Applying this model to personal protection against a virus infection, users must be aware that the risk of a virus infection exists and is significant, and can affect other people once the virus is spread from the host. Once a user is aware of said risk, they can prevent themselves from infection by implementing security measures.

The Health Belief Model is used to determine how likely one is to use preventive measures. These behaviors "are more likely to take place when the perceived severity of damage, susceptibility, and perceived benefits are high, while the costs of behavioral changes are low" (qtd. in Mariani and Zappalà 54). Applying this model our topic, users are likely to adopt preventive behaviors once they realize an infection can be avoided by successfully implementing security measures. Users should know that the risk is great, their behavior change will not come at cost, and the results of said change are highly beneficial.

Procedures and Methodology

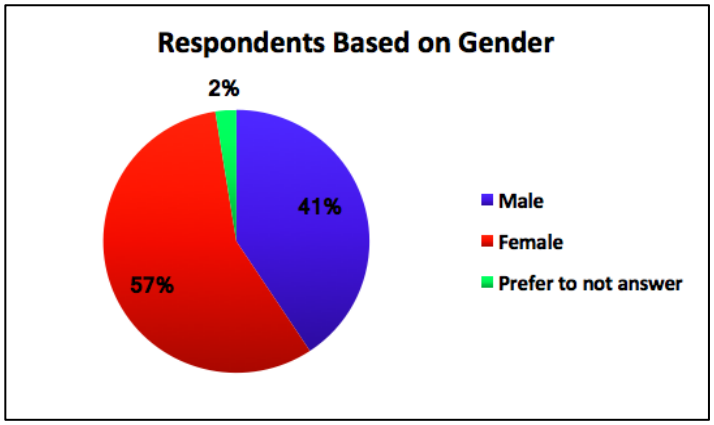
We created a survey, titled *Understanding Our Role in the Spread of Computer Viruses*. It included thirty-three questions meant to investigate how much or how little the public is educated about computer viruses and how they are unknowingly spread. The

survey asks respondents questions corresponding to the following categories: personal use of computers and external media, downloading software and opening email, experience with viruses and antivirus software, opinions on the public's knowledge on viruses, and opinions on encouraging a change in someone else's behavior. These specific questions are mentioned in the analysis of our results.

Results and Analysis

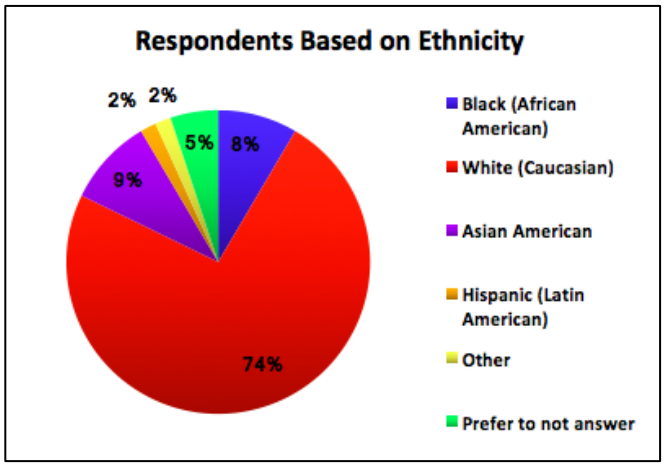
During the period of data collection, a total of 118 responses were collected. The following graphs display data for each survey question.

1. Respondents Based Upon Gender



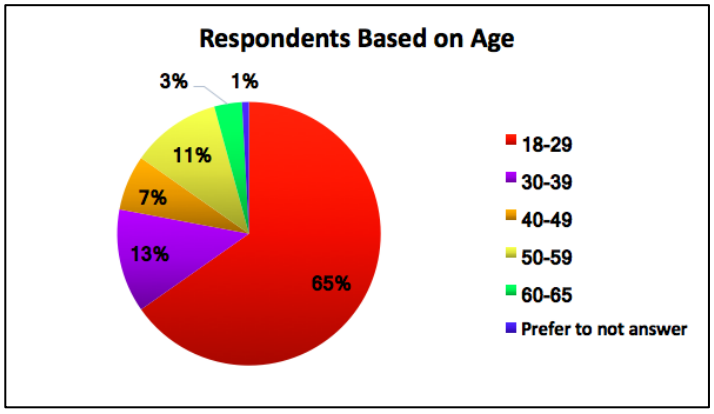
Male	48
Female	67
Other	0
Prefer to Not Answer	3
Total	118

2. Respondents Based Upon Ethnicity



Black (African American)	10
White (Caucasian)	87
Asian American/Pacific Islander	11
Native American	0
Hispanic (Latin American)	2
Other	2
Prefer to Not Answer	6
Total	118

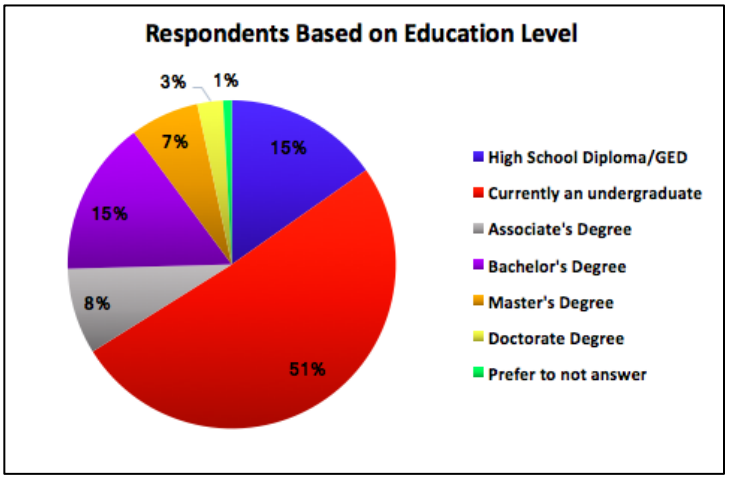
3. Respondents Based Upon Age



18-29	77
30-39	15
40-49	8
50-59	13
60-65	4

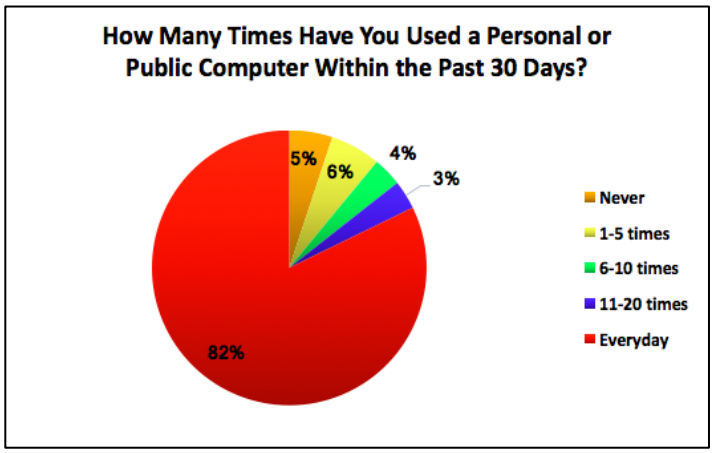
Prefer to Not Answer	1
Total	118

4. Respondents Based Upon Education Level



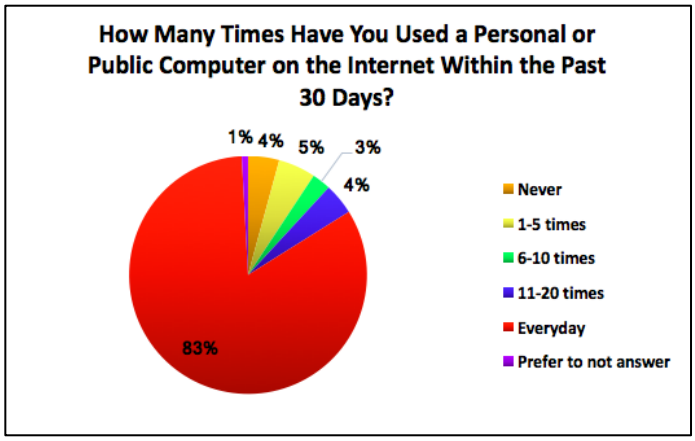
High School Diploma/GED	18
Currently an Undergraduate	60
Associate's Degree	10
Bachelor's Degree	18
Master's Degree	8
Doctorate Degree	3
Prefer to Not Answer	1
Total	118

5. How Many Times Have You Used a Personal or Public Computer Within the Past 30 Days?



18-29	77
30-39	15
40-49	8
50-59	13
60-65	4
Prefer to Not Answer	1
Total	118

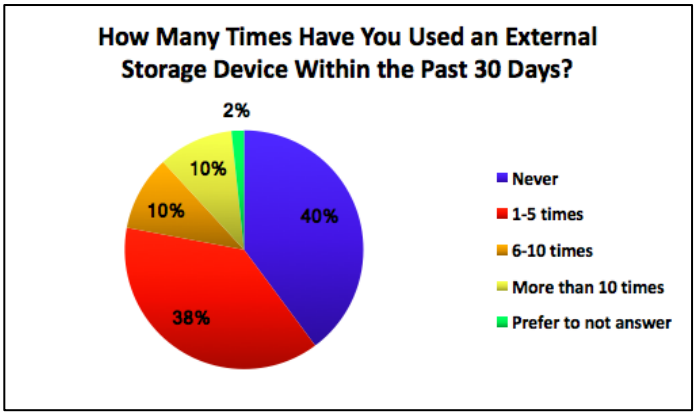
6. How Many Times Have You Used a Personal or Public Computer on the Internet Within the Past 30 Days?



Never	5
1-5 times	6

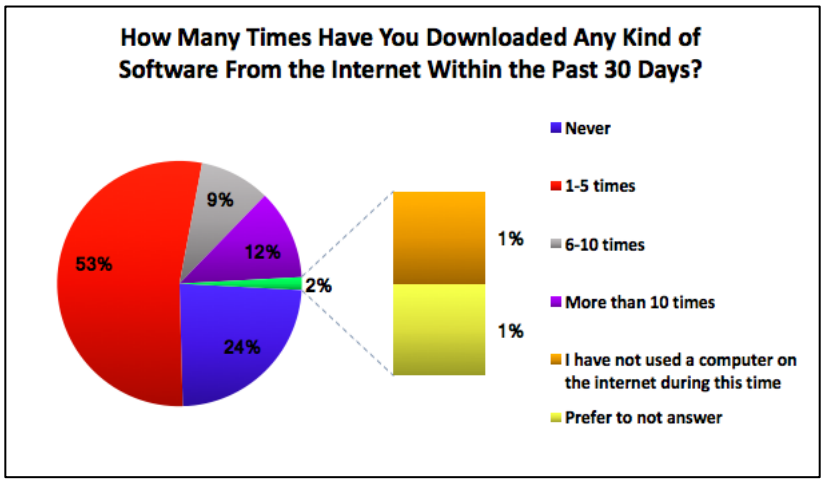
6-10 times	3
11-20 times	5
Everyday	98
Prefer to Not Answer	1
Total	118

7. How Many Times Have You Used an External Storage Device Within the Past 30 Days?



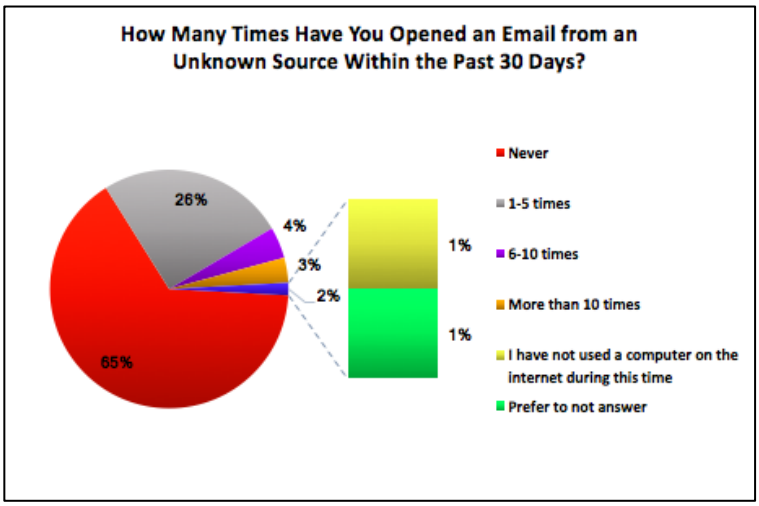
Never	47
1-5 times	45
6-10 times	12
More than 10 Times	12
Prefer to Not Answer	2
Total	118

8. How Many Times Have You Downloaded Any Kind of Software From the Internet Within the Past 30 Days?



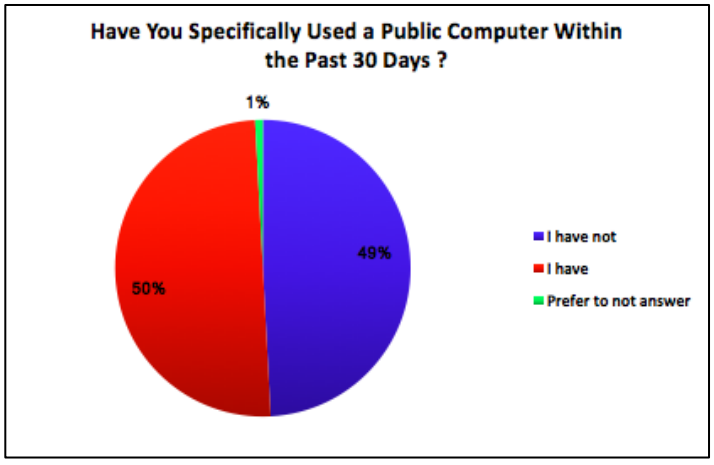
Never	28
1-5 times	63
6-10 times	11
More than 10 Times	14
I Have Not Used a Computer on the Internet During This Time	1
Prefer to Not Answer	1
Total	118

9. How Many Times Have You Opened an Email from an Unknown Source Within the Past 30 Days?



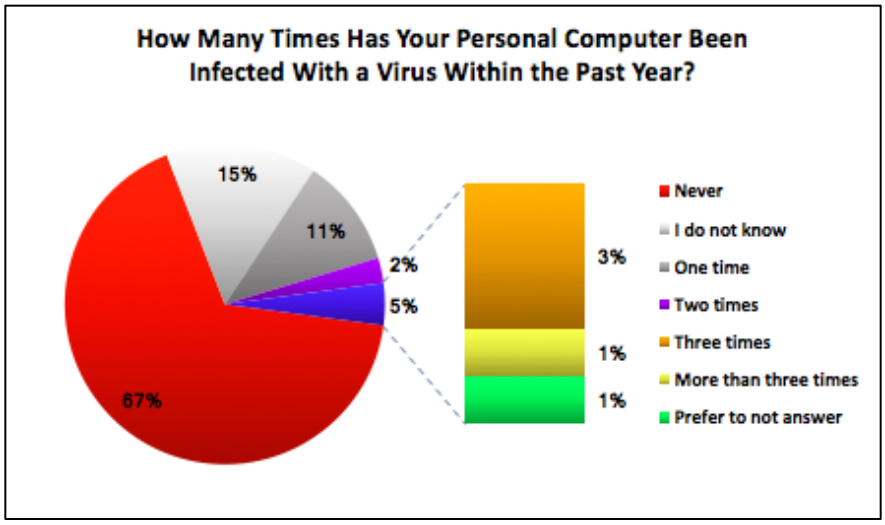
Never	77
1-5 times	30
6-10 times	5
More than 10 Times	4
I Have Not Used a Personal Computer on the Internet During This Time	1
Prefer to Not Answer	1
Total	118

10. Have You Specifically Used a Public Computer Within the Past 30 Days?



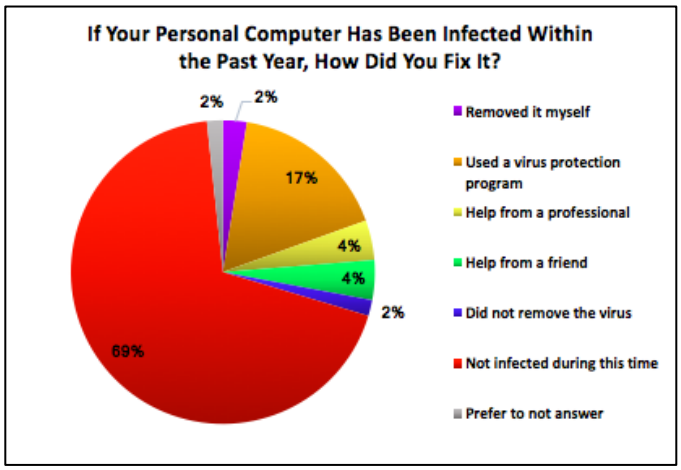
I Have Not Used a Public Computer During This Time	58
I Have Used a Public Computer During This Time	59
Prefer to Not Answer	1
Total	118

11. How Many Times Has Your Personal Computer Been Infected With a Virus Within the Past Year?



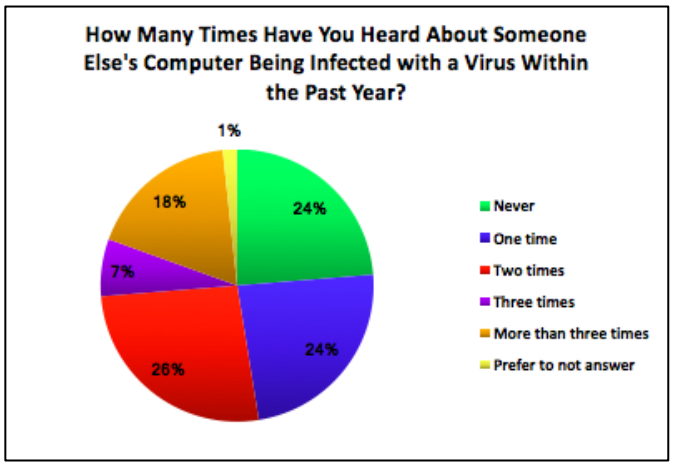
Never	79
1 time	13
2 times	3
3 times	3
More than 3 Times	1
I Do Not Know If My Computer Has Been Infected	18
Prefer to Not Answer	1
Total	118

12. If Your Personal Computer Has Been Infected Within the Past Year, How Did You Fix It?



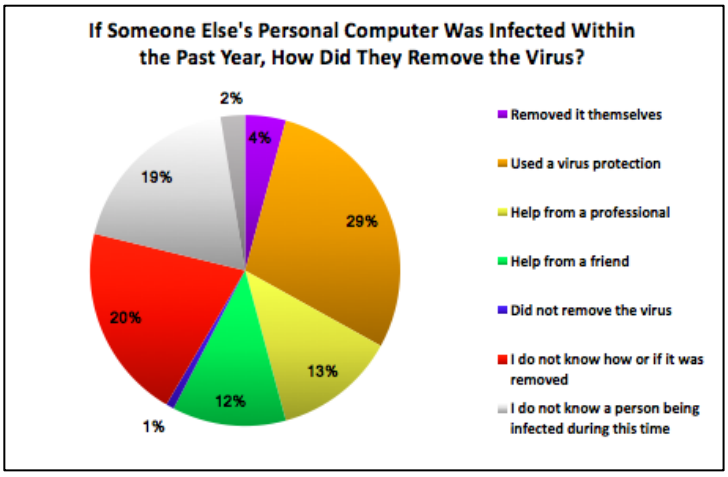
I Removed the Virus Myself	3
Used a Virus Protection Software	20
Took Computer to a Professional Business	5
Had a Friend Remove It	5
Did Not Remove the Virus	2
My Computer Has Not Been Infected During This Time	81
Prefer to Not Answer	2
Total	118

13. How Many Times Have You Heard About Someone Else's Computer Being Infected with a Virus Within the Past Year?



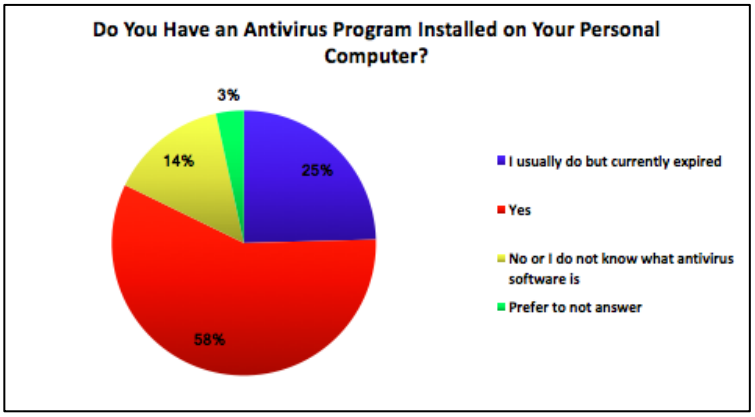
Never	28
1 time	28
2 times	31
3 times	8
More than 3 Times	21
Prefer to Not Answer	2
Total	118

14. If Someone Else's Personal Computer Was Infected Within the Past Year, How Did They Remove the Virus?



They Removed the Virus Themselves	5
Used a Virus Protection Software	34
Took Computer to a Professional Business	15
Had a Friend Remove It	14
Did Not Remove the Virus	1
I Do Not Know How or If They Removed the Virus	24
I Have Not Heard About Another Infection During This Time	22
Prefer to Not Answer	3
Total	118

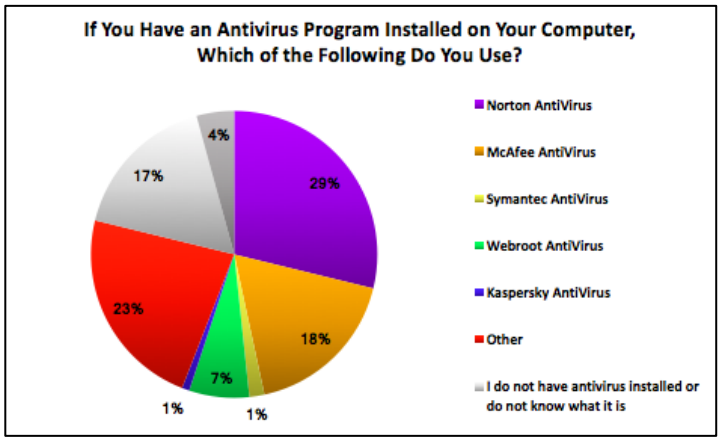
15. Do You Have an Antivirus Program Installed on Your Personal Computer?



I Always Have the Most Recent Version	29
I Usually Do But Software Has Expired	68
Currently Do Not Have Antivirus Installed	17

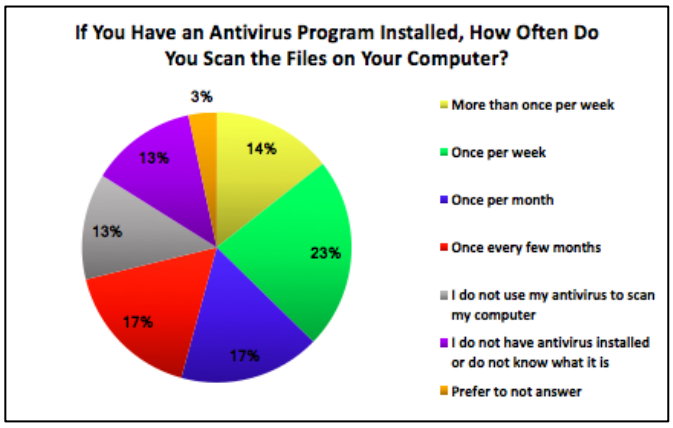
Prefer to Not Answer	4
Total	118

16. If You Have an Antivirus Program Installed on Your Personal Computer, Which of the Following Do You Use?



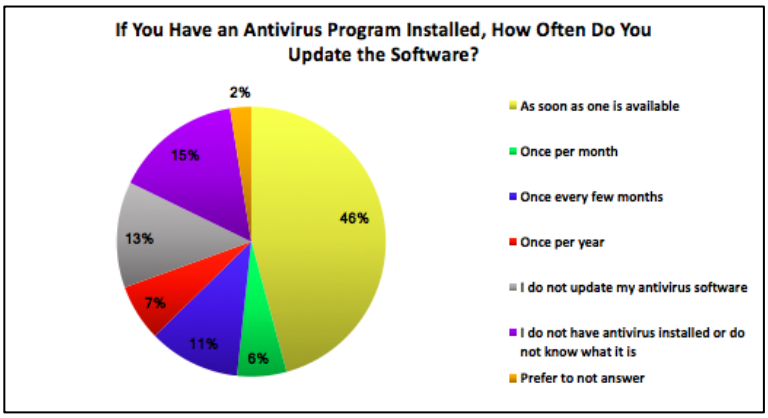
Norton AntiVirus	34
McAfee AntiVirus	21
Symantec AntiVirus	2
Webroot AntiVirus	8
Bitdefender AntiVirus	0
Kaspersky AntiVirus	1
Other	27
I Currently Do Not Have Antivirus Installed	20
Prefer to Not Answer	5
Total	118

17. If You Have an Antivirus Program Installed, How Often Do You Use it to Scan the Files on Your Computer?



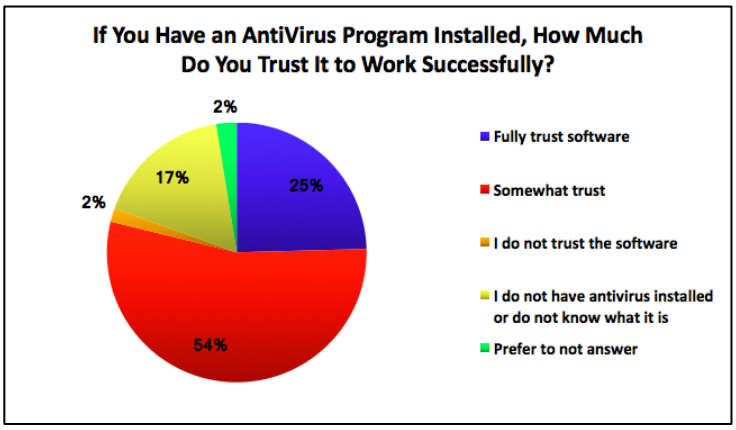
More than Once per Week	17
Once per Week	27
Once per Month	20
Once Every Few Months	20
Once per Year	0
I Do Not Scan My Files With Antivirus Software	15
I Currently Do Not Have Antivirus Installed	15
Prefer to Not Answer	4
Total	118

18. If You Have an Antivirus Program Installed, How Often Do You Update the Software?



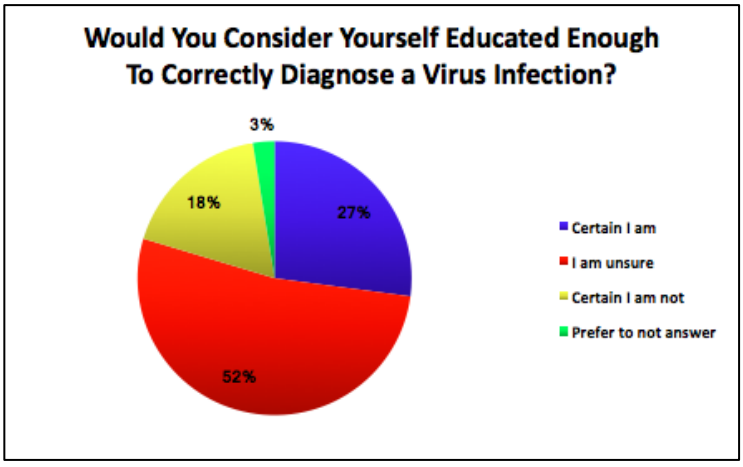
As Soon as an Update Becomes Available	54
Once per Month	7
Once Every Few Months	13
Once per Year	8
I Do Not Update My Antivirus Software	15
I Currently Do Not Have Antivirus Installed	18
Prefer to Not Answer	3
Total	118

19. If You Have an Antivirus Program Installed, How Much Do You Trust It to Work Successfully?



I Fully Trust It	29
I Somewhat Trust It	64
I Do Not Trust It	2
I Currently Do Not Have Antivirus Installed	20
Prefer to Not Answer	3
Total	118

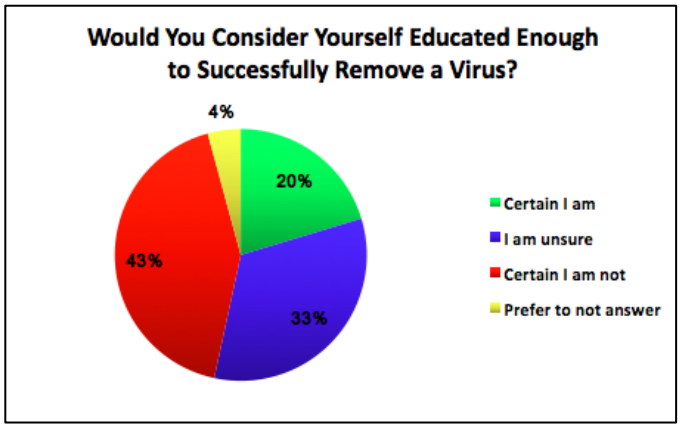
20. Would You Consider Yourself Educated Enough to be Able to Correctly Diagnose a Virus Infection?



Yes	32

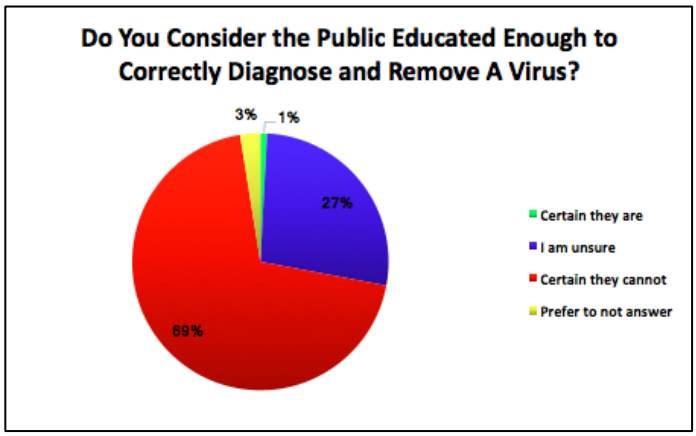
Unsure If I Can	62
No	21
Prefer to Not Answer	3
Total	118

21. Would You Consider Yourself Educated Enough to Successfully Remove a Virus?



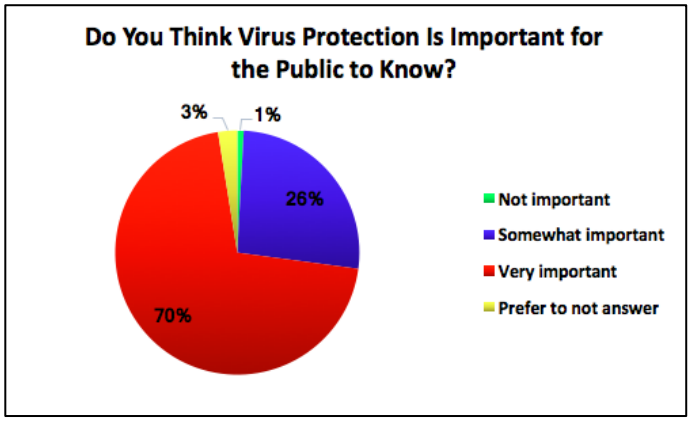
Yes	24
Unsure If I Can	39
No	50
Prefer to Not Answer	5
Total	118

22. Do You Consider the Public Educated Enough to Correctly Diagnose and Remove a Virus?



Yes	1
Unsure If They Can	32
No	82
Prefer to Not Answer	3
Total	118

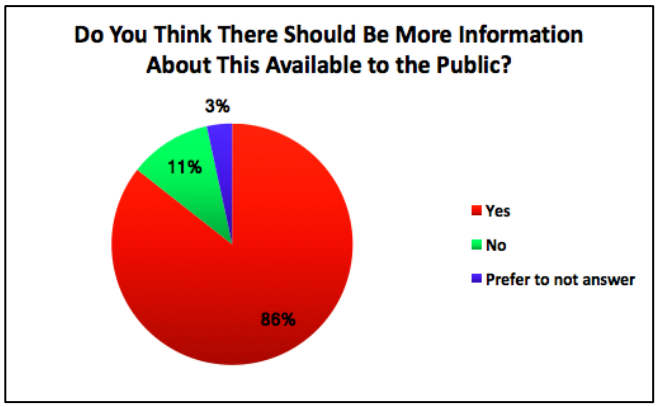
23. Do You Think Virus Protection is Important for the Public to Know?



Very important	23
Somewhat important	47
Not important	1
Prefer to Not Answer	6

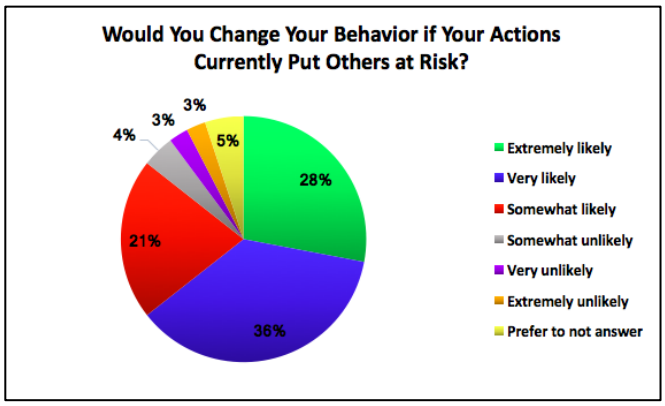
Total	118

24. Do You Think There Should Be More Information About This Available to the Public?



Yes	101
No	13
Prefer to Not Answer	4
Total	118

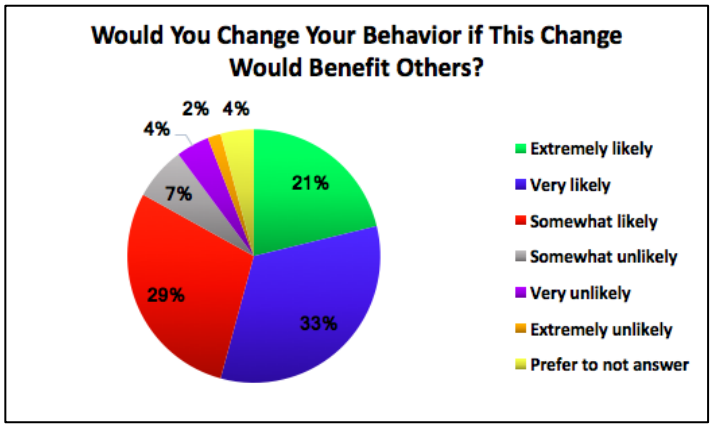
25. Would You Change Your Personal Behavior If Your Actions Currently Put Others at Risk?



Extremely Likely	33
Very Likely	43
Somewhat Likely	25
Somewhat Unlikely	5

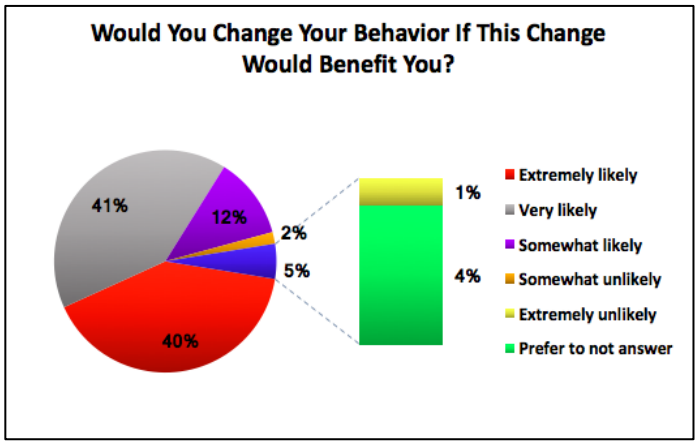
Very Unlikely	3
Extremely Unlikely	3
Prefer to Not Answer	6
Total	118

26. Would You Change Your Personal Behavior If This Change Would Benefit Others?



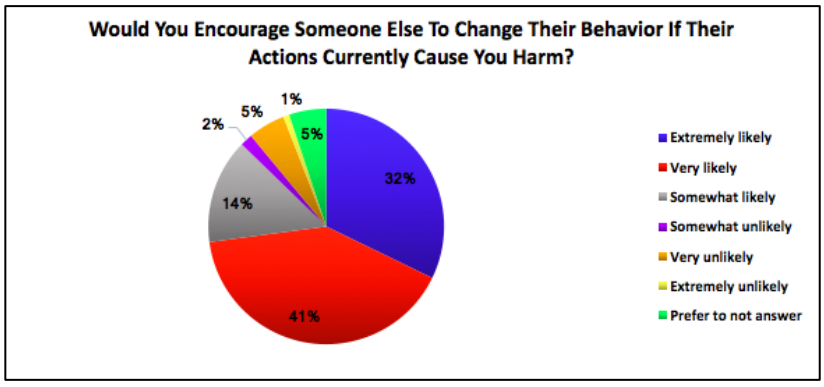
Extremely Likely	25
Very Likely	39
Somewhat Likely	34
Somewhat Unlikely	8
Very Unlikely	5
Extremely Unlikely	2
Prefer to Not Answer	5
Total	118

27. Would You Change Your Personal Behavior If This Change Would Benefit You?



Extremely Likely	48
Very Likely	48
Somewhat Likely	14
Somewhat Unlikely	2
Very Unlikely	0
Extremely Unlikely	1
Prefer to Not Answer	5
Total	118

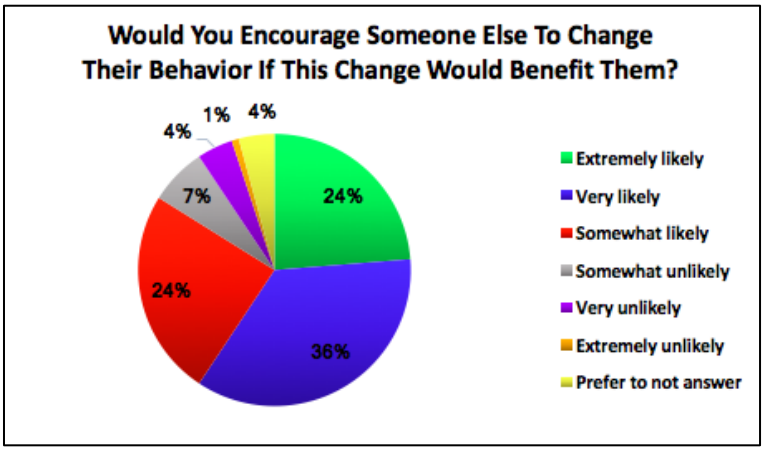
28. Would You Encourage Someone Else to Change Their Behavior If Their Actions Currently Cause You Harm?



Extremely Likely	38
Very Likely	48
Somewhat Likely	17
Somewhat Unlikely	2

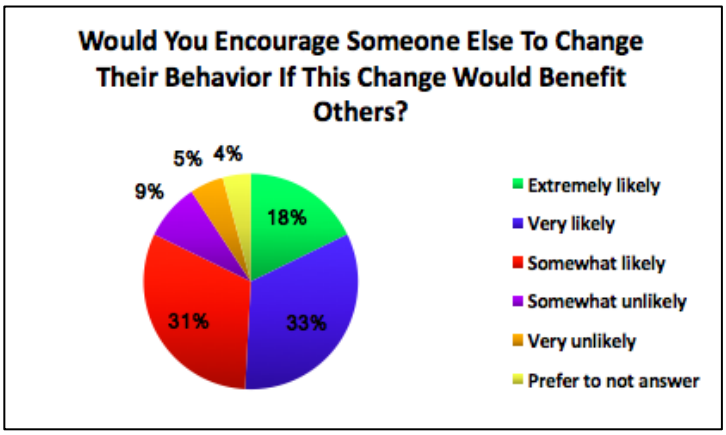
Very Unlikely	6
Extremely Unlikely	1
Prefer to Not Answer	6
Total	118

29. Would You Encourage Someone Else to Change Their Behavior If This Change Would Benefit Them?



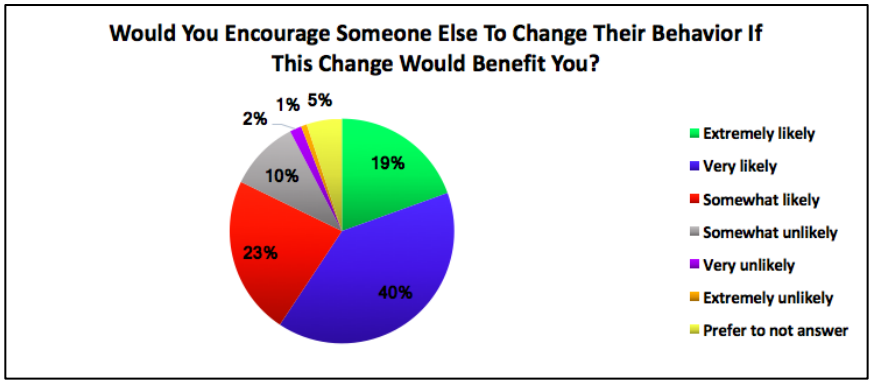
Extremely Likely	28
Very Likely	42
Somewhat Likely	29
Somewhat Unlikely	8
Very Unlikely	5
Extremely Unlikely	1
Prefer to Not Answer	5
Total	118

30. Would You Encourage Someone Else to Change Their Behavior If This Change Would Benefit Others?



Extremely Likely	21
Very Likely	39
Somewhat Likely	37
Somewhat Unlikely	10
Very Unlikely	6
Extremely Unlikely	0
Prefer to Not Answer	5
Total	118

31. Would You Encourage Someone Else to Change Their Behavior If This Change Would Benefit You?



Extremely Likely	23
Very Likely	47
Somewhat Likely	27

Somewhat Unlikely	12
Very Unlikely	2
Extremely Unlikely	1
Prefer to Not Answer	6
Total	118

32. Would You Encourage Someone Else to Change Their Behavior If You Knew Their Actions Currently Harm Others?

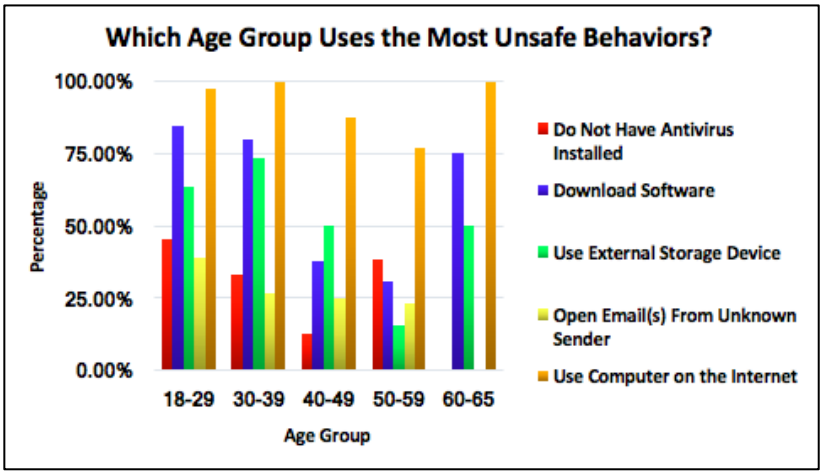
Extremely Likely	32
Very Likely	48
Somewhat Likely	20
Somewhat Unlikely	4
Very Unlikely	5
Extremely Unlikely	4
Prefer to Not Answer	5
Total	118

We break down our results into the following three major analyses based on the age groups of respondents: the group putting us most at risk for infection, the group most likely to cause behavior change, and the group knowing the most about diagnosing and removing viruses. We recall the results from question three of the survey:

18-29	77
30-39	15

40-49	8
50-59	13
60-65	4
Prefer to Not Answer	1
Total	118

Analyzing the age groups to determine which puts us most at risk for infection, we determine the percentage of respondents in said grouping that claim to use each of the following risky behaviors: not having an antivirus program installed on their personal computer, frequently downloading software, frequently using an external storage device, opening email(s) from an unknown sender, and frequently using a computer on the internet. These behaviors are analyzed because they are common among users of all ages.



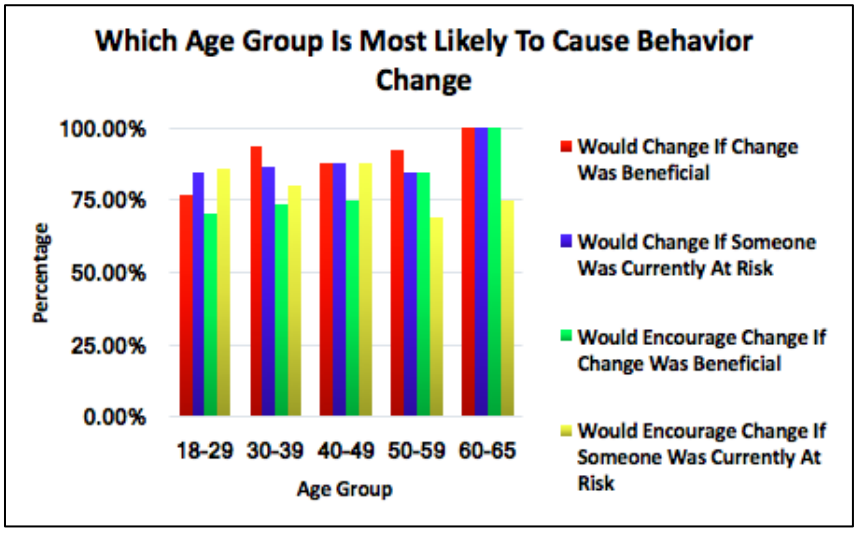
	18-29	30-39	40-49	50-59	60-65
Do Not Have Antivirus Installed	45.45%	33.33%	12.50%	38.46%	0.00%
Download Software	84.41%	80.00%	37.50%	30.76%	75.00%
Use External Storage Device	63.63%	73.33%	50.00%	15.38%	50.00%
Open Email(s) From Unknown Sender	38.96%	26.67%	25.00%	23.07%	0.00%
Use Computer on the Internet	97.40%	100.00%	87.50%	76.92%	100.00%
Average	65.97%	62.66%	42.50%	36.98%	45.00%

An average percentage of respondents having these behaviors is calculated, determining which age group has the highest percentage of respondents having these

risky behaviors. On average, 18-29-year-old respondents have the riskiest behavior and put us more at risk for infection (65.97%), while 60-65-year-old respondents use the safest behavior while on their computers (45%). Comparing the age groups' average percentage, there is a downward trend from 18-29-year-olds to 50-59-year-olds with an upward trend between 50-59-year-olds and 60-65-year-olds. The most common behavior among our respondents is frequently using a computer on the internet, while the least common behavior is opening email(s) from unknown senders.

Since many respondents claim to frequently be on the internet, we should release more information about viruses and personal protection online. Having this information readily available to these consumers can contribute to future behavior change.

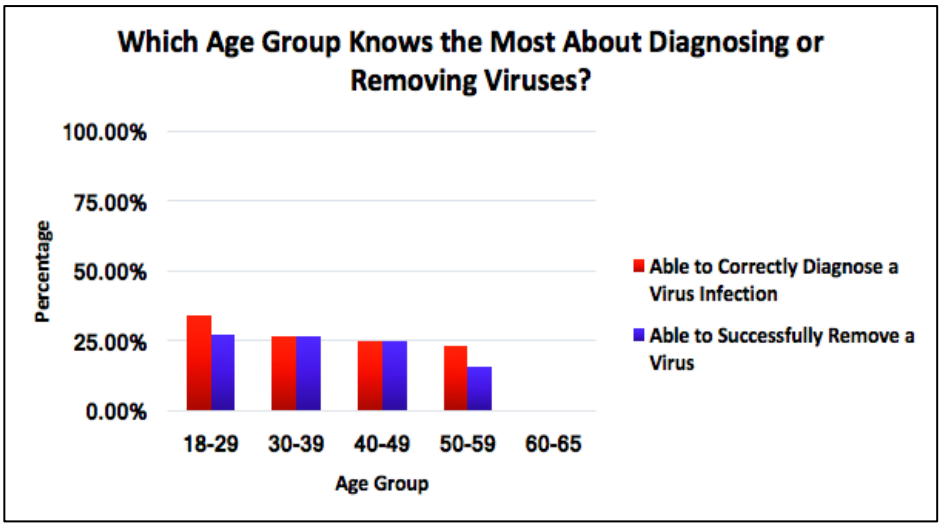
Analyzing the age groups to determine which is most likely to cause behavior change, we determine the percentage of respondents in said grouping that claim they believed they would at least be 'somewhat likely' to change their behavior or at least 'somewhat likely' encourage behavior change in another depending on the given situation.



	18-29	30-39	40-49	50-59	60-65
Would Change If Change Was Beneficial	76.62%	93.33%	87.50%	92.30%	100.00%
Would Change If Someone Was Currently at Risk	84.41%	86.67%	87.50%	84.61%	100.00%
Would Encourage Change If Change Was Beneficial	70.12%	73.33%	75.00%	84.61%	100.00%
Would Encourage Change If Someone Was Currently at Risk	85.71%	80.00%	87.50%	69.23%	75.00%
Average	79.22%	83.33%	84.38%	82.69%	93.75%

An average percentage is calculated for each age group to determine which has the highest percentage of respondents with these opinions. On average, 60-65-year-old respondents promote behavior change the most (93.75%), while 50-59-year-old respondents promote such change the least (82.69%). Comparing the age groups' average percentage, there are upward trends between 18-29-year-olds and 40-49-year-olds and also between 50-59-year-olds and 60-65-year-olds, with a downward trend between 40-49-year-olds and 50-59-year-olds.

Analyzing age groups to determine which knows the most about diagnosing and removing viruses, we determine the percentage of respondents in said grouping that claim they are certain they can successfully diagnose or remove a computer virus.



	18-29	30-39	40-49	50-59	60-65
Able to Correctly Diagnose a Virus Infection	33.77%	26.67%	25.00%	23.08%	0.00%
Able to Successfully Remove a Virus	27.28%	26.67%	25.00%	15.39%	0.00%
Average	30.53%	26.67%	25.00%	19.24%	0.00%

An average percentage is calculated for each age group, determining which has the highest percentage of respondents with these skills. On average, 18-29-year-old respondents have these skills the most often (30.52%), while 60-65-year-old respondents have these skills the least often (0.00%). Comparing the average percentage of the age groups, there is a downward trend between 18-29-year-olds and 60-65-year-olds. Based on this, we must find a way to educate all users on virus detection and removal, especially older generations (50-65-year-olds).

Each age group has an alarming percentage of users who claim they are unable to successfully diagnose and remove a computer virus. These users, if infected, can spread a virus to others if they cannot notice symptoms of infection on their computer.

Inaccurate Data

All data recorded and displayed in this paper is representative of our sample population, not all users of a given category. To be more specific, our results analysis above includes misleading data for the category of 60-65-year-old respondents. For our survey to include data that is less misleading, we need a larger sample size, or more responses from individuals between 40 and 65-years-old. Data recorded for 60-65-year-olds using unsafe behaviors is misleading because 0.00% of respondents in that category claim to not have antivirus installed on their personal computer while also not opening email(s) from unknown senders. This result is certainly false because it is not possible for zero percent of this population to not partake in said risky behaviors. Data recorded for

60-65-year-old users causing behavior change is misleading because not all users in this category will share the same opinion on behavior change as our respondents. Data recorded for 60-65-year-old respondents knowing how to correctly diagnose and remove a virus is misleading because it is not possible for zero percent of this population to lack these skills.

Comparing with Other Surveys

Compared to results from the survey conducted by Divya Singhal in India, their respondents are more likely to have antivirus software installed and update it more frequently than our respondents (28). The two surveys ask similar questions and here we compare the results of both.

Their survey asks respondents about their experience "in eradicating virus problems", and a majority "prefer to solve the virus problems themselves and succeeded doing it" (Singhal 27). To be exact, 33% of their respondents claimed to solve the problem themselves while 58% of respondents had someone aid in their virus removal and 4% ignored the problems (Singhal, 27). Very few of our respondents claim to fix the infection themselves or even seek assistance. To be exact, 2% of our respondents claimed to remove the virus, while 8% had assistance from either a friend or a professional. Two percent of our respondents claimed to ignore the issue and not remove the virus from their computer.

Another question in this survey analyzes "the respondent's awareness towards the antivirus functionality and capabilities" (Singhal, 27). Results show that "[m]ajority of respondents . . . were confident that their antivirus software was capable to clean viruses

found on their machine" and "have antivirus software installed on their machine" (Singhal, 27). Most of our respondents (58%) currently have antivirus software installed on their personal computer, but only 43% of those with antivirus software fully trust the program to resolve their infection. Many respondents who claim to have antivirus software installed on their personal computer also claim to only somewhat trust their software to successfully detect or remove a virus on their system.

Both surveys also have a question investigating how often respondents update their antivirus software. Over 90% of "the respondents [update] their antivirus monthly" and "5% never [update their software]" (Singhal 28). More than half (52%) of our respondents with antivirus software installed claim to update their software at least once per month. A staggering 13% of respondents with an antivirus package installed claim to never update their software.

The last question from this survey we will compare is based on whether respondents are interested in having more "knowledge of viruses and antivirus [software]" (Singhal 29). Exactly "98[%] of the respondents were very much interested" in such knowledge. When asked, 96% of our respondents claim that virus protection is at least somewhat important for the public to know more about. To be more specific, 70% of respondents believe this topic is very important for the public to be more educated about.

Conclusion

Based on our collected survey results, we can conclude that today's users are using unsafe behaviors while operating their computers but they are also willing to

rehabilitate such behaviors. We can speculate that users will continue to operate recklessly because they do not perceive a high risk of infection. To change this, developers should work to create software that influences users to work under the security measures in place. The greater risk that is perceived by users, the more secure behaviors they will use while operating their computers.

Overall, respondents believe that the topics of computer viruses and personal protection from such are very important for the public to be informed about. The positive response leads us to believe that people are concerned about the potential risk of being infected by a computer virus. A vast majority of respondents also believe that more information about this topic should be available. The more information we can give our concerned citizens, the safer we will be in the future. Until then, we will remain an unsecure population who risks losing personal data because we are either ignorant of or relentlessly against measures meant to keep us safe.

Future Directions

After analyzing our data, two main question arises: "If respondents claim to promote behavior change if people are at risk, why are they not encouraging others to change their hazardous behavior for protection against viruses?" and "How comfortable are respondents with the security methods they currently use?". To better investigate these questions, we would release another survey. With this new information, we can begin to bridge the gap between users and developers to create a more secure cyber community.

Works Cited

Bo, Zhang, Li Qianmu, and Ma Yuanyuan. "Research on Dynamic Heuristic Scanning Technique and the Application of the Malicious Code Detection Model." *Information Processing Letters* 117 (2017): 19-24. *EBSCOhost*. Web. 13 Mar. 2017.

"Cyber Risk Manager Sees Attacks Spreading." Interview by Donna Mahoney. *Business Insurance* 15 Feb. 2016: 12. *EBSCOhost*. Web. 15 Mar. 2017.

Mariani, Marco G., and Salvatore Zappalà. "PC VIRUS ATTACKS IN SMALL FIRMS: EFFECTS OF RISK PERCEPTIONS AND INFORMATION TECHNOLOGY COMPETENCE ON PREVENTIVE BEHAVIORS." *TPM: Testing, Psychometrics, Methodology in Applied Psychology* 21.1 (2014): 51-65. *EBSCOhost*. Web. 13 Mar. 2017.

Pfleeger, Shari Lawrence, and Deanna D. Caputo. "Leveraging Behavioral Science to Mitigate Cyber Security Risk." *Computers & Security* 31.4 (2012): 597-611.Web.

Salomon, David. *Elements of Computer Security*. New York: Springer-Verlag, 2010. Print.

Singhal, Divya. "Computer Viruses in India-A Questionnaire Survey." *International Journal of Computer Applications* (n.d.): 26-32. *EBSCOhost*. Web. 4 Apr. 2017.

SPECTOR, LINCOLN. "Spot the Telltale Signs of Malware on Your Computer." *Pcworld*, vol. 33, no. 2, Feb. 2015, p. 27. *EBSCOhost.* Web. 20 Mar. 2017.

SurveyMonkey. "Are My Survey Responses Anonymous and Secure?" *Are My Survey Responses Anonymous and Secure?* N.p., n.d. Web. 05 Dec. 2016.

SurveyMonkey. "How Do I Break down My Survey Results?" *How Do I Break down My Survey Results?* N.p., n.d. Web. 5 Dec. 2016.

SurveyMonkey. "Opening & Closing Surveys." *Opening & Closing Surveys*. N.p, n.d. Web. 05 Feb. 2017.

Zhang, Xulong. "Modeling the Spread of Computer Viruses under the Effects of Infected External Computers and Removable Storage Media." *International Journal of Security and Its Applications* 10.3 (2016): 419-28. *EBSCOhost*. Web. 20 Mar. 2017.