THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

COLLEGE OF INFORMATION SCIENCES AND TECHNOLOGY

PERCEPTIONS OF SMARTPHONE SECURITY

KEVIN LAUBSCHER
SPRING 2014

A thesis
submitted in partial fulfillment
of the requirements
for a baccalaureate degrees
in Security and Risk Analysis and Applied Statistics
with honors in Security and Risk Analysis

Reviewed and approved* by the following:

Anna Squicciarini
Assistant Professor of Information Sciences and Technology
Thesis Supervisor

Peng Liu
Professor of Information Sciences and Technology
Honors Adviser

* Signatures are on file in the Schreyer Honors College.

ABSTRACT

Smartphones are becoming very popular in today's society, but is the popularity of security options and safety growing along with it? This study explores the average college student's perception of smartphone security. I will be examining the respondent's use, safety and security devices on both laptop/desktops and smartphones. The participating students were sampled from a large northeastern university and were asked to complete an online survey. The data was examined using statistical analyses to see if the average college student will rate their level of security on laptops/desktops higher than that on their smartphones. I will be looking at many factors including, gender, school year, history of computer security incident, level of computer knowledge and level of risk tolerance. If a relationship is found to exist, this study can be used as initial evidence that more education and training on smartphone security is necessary.

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGEMENTS

I would like to thank all of my professors in the College of Information Sciences and Technology and the Department of Statistics. It has been through their teachings that I started and maintained an interest in smartphone security and statistics. I would especially like to thank Anna Squicciarini for helping me through the thesis process. I would also like to thank Peng Liu and Lisa Lenze for all of their advising help. Finally I would like to thank my family, especially my parents David and Linda Laubscher, for supporting me throughout my four years at Penn State.

Chapter 1

Purpose for Research Study

Smartphones are a large part of society today which highlights the need to consider the importance of smartphone security in one’s daily life. According to Mintel’s report on mobile phones in the US, 2012 saw mobile phone sales reach $37,996 million. They have forecasted sales to continue to increase and reach $48,287 million in 2017. Of users with mobile phones, 48% use email and 43% use the Internet on their phones (Hulkover, 2013). Surfing the Internet and checking email from unknown sources without the proper security is a major vulnerability to an individual’s private personal information and ease of completing day to day tasks. Users need to keep their personal information such as credit card information private to avoid identity theft and other troubles. They also should be aware of the security options available to help prevent theft.

In this study I will be looking at smartphone and laptop owner’s current usage and perceived safety on each device. I am also going to look at security options the respondents are currently using or have enabled on their devices. The key variable I will be studying is perceived security which is defined as the safety and comfort level one feels while using each device. Even though users perform similar functions on both laptops and smartphones, the purpose of the study will be to see if they have similar security perceptions and functions.

Through my research, I hope to show that many people are unaware of the vulnerability of unsecured smartphones. In this study I want to prove that users don’t view smartphones the same way they do laptops. My hope is that the field of security can view this study as a warning sign to educate people more so smartphones can be used with the same comfort as laptops. I also want to look at the impact of a person being risk adverse versus risk tolerant and someone with little computer knowledge versus someone with greater computer knowledge. I also think that people who have suffered from a computer security incident will be more likely to have stronger security. Finally, this study will also look to analyze the use and perceived security on smartphones compared to laptops/desktops. I will look to see if there are functions users are still more comfortable performing on smartphones.

Chapter 2

Smartphone Security Background

The phone has come a long way since Alexander Graham Bell's telephone in 1876. In 2007, Apple announced the visionary iPhone and Google announced the Android operating system. These two companies ushered in the age of smartphones. According to a report from The Guardian in 2012, Apple sold 4.7 million units in just its first quarter of sales (Arthur). This made up 13% of the market at that time. In 2010, Android came out with Android phones that had full touchscreens, just like Apple's iPhone. After three months the phone gained 10% of the market (Arthur).

The year 2012 saw history when a study published by Canalys showed a higher number of smartphones shipped than PCs. The shipment of smartphones grew 62.7 percent from 2011 to a total of 487.7 million compared to the 414.6 million PCs (Mogg). These numbers prove the growing popularity and use of smartphones. With this increase and subsequent change in popularity, companies need to evolve along with the market to interact with their customers. Many banks have created mobile applications to deposit checks and transfer funds. Web browsers and other applications allow users to post personal information and shop from their smartphone. To create and maintain these applications, companies spend a lot of money and man hours.

There is a lack of knowledge among the general public on the importance of smartphone security. A study conducted by AVG Technologies Inc. found "an alarmingly low percentage (of smartphone users) are aware of the security threats and lack a sufficient knowledge to protect them" (Kass, 2011). The expanding smartphone industry is going to continue to thrive with more technology and use options. People are tuning to their smartphones to complete more and more of their everyday tasks.

Chapter 3

Literature Review

Androulidakis and Kandus (2011) examined university students and how they downloaded software to their mobile phones. The study looked at two main research questions. The first one focused on how students downloaded software to mobile phones. The researchers wanted the user's to reflect on whether or not they download software and if they do, what kind of software they downloaded. The second research question asked about perceived mobile phone security. It was spilt up into two more focused questions: "are you informed about how the options and technical characteristics of your mobile phone affect its security?" and "how secure do you consider communication through mobile phones?" These questions are meant to rate user's security knowledge and awareness as it relates to mobile phones. There are many different variables that this study looks at. The main variable studied is the amount of downloading depending on many different variables. The variables measured against downloading percentage include, country, sex, bill amount, field of study, age, password protection, antivirus and backup. The method used for acquiring the information was a multiple-choice questionnaire. The face-to-face survey was chosen because it was "more accurate and has a higher degree of participation from the respondents" than e-mail questionnaires (Androulidakis and Kandus, 2011). Researchers wanted to target University students aging from 18 to 26. The questionnaire had two sections. One section contained demographic questions and mobile phone usage and qualities. The next section asked about security knowledge, practice and feeling questions. The survey concluded that users' security awareness and behavior correlate to downloading characteristics. When it came to mobile phones, 47% of the participants don't download at all. It was found that men are more actively downloading overall and especially with games and applications. An even more alarming figures was that users knew there was antivirus for their phones and still did not use it. In their concluding arguments, the researchers believe that “marketing efforts combined with educational programs to raise awareness and security” should increase.

A convenience sample is used to disseminate the survey. The researchers explain why this was the best sampling method with their circumstances. It is important to note the characteristics of the convenience sample and this study doesn’t. For example, handing out surveys in the business building would have different results than handing out surveys in the education building or in a central gathering place. One of the main criticisms I have about this article is it doesn’t account for the type of phone used by the participants. Participants with a smartphone opposed to a basic phone are going to have different possibilities and options. There are a couple of possible future areas of interest not addressed in this article. As mentioned earlier I would like to see this survey done in other areas of the world. I would be interested to see if similar results came from places like the United States. My survey will be taking place on a large Northeastern university. In addition to other locations, the researchers could have looked at the respondent’s general information technology knowledge. In all of the statistical tests the amount of downloading is always against all of the other variables. In my survey I want to test multiple breakdowns to view the different slices of data.

Zhu (2012) examined mobility patterns from several dimensions like application breakdown, device types and user roles. He also was interested in the data service usage. The main three types of data services are HTTP, MMS and SIP. One of the main research questions was whether there were differences between usage type and type of device. For example, if there was a difference between PDA phones and BlackBerry in the fraction of users that use mail applications. Another question was the difference between roaming users and their data usage. In the case of the user roles the independent variable is the type of user (roaming or local) and the dependent variable is the status of whether or not they access data. The other study looks at the usage type (mail, ringtones etc.), phone type (PDA, BlackBerry, etc.) and the number or fraction of users that use the different usage types. The researcher used one of the largest cellular network carriers in the U.S. and performed a data trace. The data trace collect any session level information for all communications that took place between any two endpoints. The trace lasted from April 16, 2009 to April 22, 2009 and contained about 2 million users. The study proved that there are major differences between certain device types and the usage type. It also showed very similar uses between laptops and PDA phones. Another conclusion from the study was the difference in data usage between local users and roaming users. 81.6% of local users accessed data whereas 8.67% of roaming users accessed data.

One of the more interesting and unique items about the study was the focus on roaming versus local users. Previous studies have not considered the difference between the two groups. The source of the data really captured the entire picture of data usage for the company. A possible problem could be with the types of phones the company allows on their network. For a long time iPhones were only allowed on the AT&T network. A study that possibly doesn't consider iPhones is losing a significant portion of smartphone users. The gathering of data only took place once for one week. It would be interested to see if anything significant occurred during that week that could have skewed the data. In order to avoid this data could have been sampled from a couple of other weeks. This may not have been available to the researcher depending on the deal with the cellular network company he was using. The main thing not addressed in this article is the aspect of security. It mostly focuses on the data usage of customers, but security could definitely be another area of interest. I think a difference in security settings between roaming and local users could be nice addition to my survey. Another future area of research could be differences in locations. The researcher could compare different time zones or urban vs. rural differences.

Allam (2009) aimed to look at the gap between a software consultancy's current overall and smartphone security and the necessary security to comply with current standards in his research. The main research question of the article is "how can a software consultancy organization measure the vulnerability gaps that exist between its existing security solution and a smartphone security solution so it conforms to both the COBIT 4.1 framework and the ISO27002 standards?" The variables in this study were the level of responsibility, and the level of importance for each item asked. The level of responsibility was broken into two categories, either an individual's job required them to be responsible for security requirements or not.

The questionnaires were given to software consultancy organizations that volunteered to participate. The researcher asks that the surveys be distributed to employees at different levels of the organization. The overall result of all the questions was examined and found to have an average of .8 which is between neutral and low importance. This supports the claim that "employees do not perceive smartphone security to be of moderate or high importance to their organization" (Allam, 2009). The average for respondents who were responsible for security was only a little higher than respondents who weren't, but both still fell in between neutral and low importance. The question that received the overall highest score was "smartphone users are aware of who owns the data processed and stored on their device" with a rounded average of 1.31.

The main limitation of this study was the distribution of the questionnaire. This sampling strategy makes it difficult to determine if the companies that volunteered for the study were representative of the larger population. Within the companies, I would have ideally set up a stratified sample to ensure all the different subgroups were surveyed instead of just asking. The Likert scale and the methods surrounding it were good. In the rating scale low importance is rated higher than neutral. I would be interested to see whether others would agree with this placement. I would think users would have a harder time choosing between neutral and low importance.

The questionnaire seemed to cover a lot about smartphone security but I think there are other slices to be made from the data. I think that looking at differences in age groups would be very interesting. It could be possible that the younger technology-savvy employees know more about security or that the older employees have learned from experience. A comparison between the gender of employees and the perception of security could yield results. The future research that is most clear is expanding this study to businesses other than software consultancies. Almost all businesses use smartphones to improve day-to-day and overall operations. Security in all these organizations is important and should be measured.

Felt's (2012) research topic focused on the security of smartphones and the third-party applications that users can install on them. Malicious application creators can use the resources the applications need to steal personal information or gain access to certain parts of a smartphone. The first research question asked users about their level of concern when it came to 99 risks about smartphones. The second question asked users to judge their reactions to different warning messages. The independent variables in this study were the 99 different smart phone risks the researchers came up with. These risks covered a wide range of smart phone features and situations. The dependent variable is the user's opinion on the severity of the risk. The researchers used two methods to gather data. The first was a survey that asked users about their opinions on apps performing certain tasks without user approval. The second method was an opened survey to gather more rich data about certain risks. The risks that ranked the highest in user concern all dealt with permanent data loss or financial loss. Risks that ranked the lowest in user concern dealt with phone settings or the sending data to servers without permission. An interesting item that came out of the open ended discussion was that some users held service providers responsible for malicious applications. This is interesting because service providers have no control on the applications the user decides to install on his smart phone.

The main limitation of this study was the representativeness of the population. The sample seemed to contain people with a greater knowledge in technology. The people who frequent Mechanical Turk may be more familiar with computers and have more years of education. The VUR rating needed more explanation and backing. There was no description of why the researcher chose it over other ratings. A better measure would allow a score that meant something by itself not just against other risks. Future research in this area should ask users about security on their phone. The whole survey alerts users to the main things malicious applications can perform without consent from the user but has no measure of any preventive techniques. The study I am completing will measure if the user has taken any measures to become more secure and to stop some of the things this research mentioned.

Mashevsky (2005) explores the growth of malware. Malware is any virus, worm, rootkit or malicious code that does harm to computer or network system. The two research questions of this study are “what makes you open suspicious messages?” and “how often do you update your security solution?” These questions are important because they get at the greatest weakness in any security plan, the users. The first variable is reason for opening email. The second variable in this study are the time of update. The researcher mentions that it was a Kaspersky Lab user poll which doesn’t tell the reader much. It is also stated that the survey took place online. The first question yielded interesting information on why users open suspicious email. Only 55.2% of the people surveyed said that they never open suspicious email, leaving 44.8% vulnerable to attacks. The biggest reason why people opened the messages is because of curiosity. The second question dealt with the speed at which users update their security. The Internet poll found that only 14.6% of users update daily and 10.3% after an update is released. At the current rate of zero-day vulnerabilities updating after either of these two times leaves the user vulnerable to attack and infection.

The main limitation of this article that I have identified relates to the selection of the participants and dissemination of the survey. The article doesn’t address either of these issues. The reader has no idea whether the sample was a fair representation of the population. There is no mention of how the participants were chosen or found out about the survey. I would assume this was a convenience sampling and data on the sample representing the population is needed. In order to improve this article the researcher could analyze more risky behaviors. The only one represented in the paper is suspicious email. There are other actions like visiting suspicious webpages or entering personal information into sites that could be looked at further. Analyzing these behaviors or ones like it can give the reader a better look into the reasons why average users perform risky behaviors.

The articles discussed above reviewed provided an overall picture of smartphones. The articles all used some sort of self-report method and most were convenience samples. The different articles have all used different scales and ways to measure the knowledge of security. By looking at the strengths and weakness of each, I can shape my scale and survey based on what is best. In Allam’s (2009) research he used a scale from “-2” meaning not very important to “3” meaning very important. Most scales were not like this and I thought it was interesting how the scale was not even on both sides. Overall users seem unaware of the potential threats. Felt’s (2012) research showed that users are not happy with certain problems that are due to a lack of security. Allam (2009) showed that even a highly-technical company like a software consultancy did not view security in a high enough regard. The articles I reviewed above have shown that the average user is unaware of the necessity of security overall. Given that smartphone security it is such a new problem, there is not much research on it. This study will bring to light the problem with everyday user’s perception of security.

Chapter 4

Study Methodology

Participants

To define my anticipated sample, I will first define my population. For the ease of sampling, the population will be college students at a large northeastern state university. The sample was a large number of students across all years of study. The students were from Penn State University. In the 2013/2014 school year, Penn State has an undergraduate population of about 35,000 students with degrees across twelve different academic colleges.

Procedure

The survey was constructed using the online tool, Qualtrics. Qualtrics is a university-approved survey software that allows the user to easily create, disseminate and collect results for surveys. The survey was distributed through an online link. The link was given to students via list-serve emails and class Facebook pages. The survey was active for a week from February 4, 2014 to February 11, 2014. A successful completion of the survey was defined as answering all the questions given as well as stating “Yes” to the questions, “Do you own a Smartphone?” and “Do you own a Laptop or Desktop Computer?” Out of the 85 responses to my survey, there were 66 students that successfully completed the survey.

Measures

The survey was divided into six sections (the full survey can be found in Appendix A). The first page contained information about the survey itself and served to ensure the responder was providing informed consent. The second page contained questions related to demographic information. The respondent was asked for their gender, year, whether they owned a smartphone and a desktop and if they were ever the victim of a computer security incident. The next page contains two groups of questions to derive the respondent's level of computer knowledge and risk aversion/ tolerance. The questions on both of these last two pages will be used to further breakdown the overall objectives discussed later in this section.

The next page is about laptop/desktop and smartphone usage. In order to measure how safe students feel performing different actions of each device, it is important to understand what students use each device for. This section asks the respondent to report how often they use six different functions of a laptop/desktop and then a smartphone. The six functions are online banking, social networking, Internet surfing, email, online gaming and e-commerce (shopping). The question asks "I often perform the following actions will using each device" and uses a Likert scale ranging from strongly agree to strongly disagree to answer. In this question, I want to see if there is a difference in the amount that students use each function on a smartphone versus a laptop/ desktop.

Using the same six functions as the last section, this section asks the user to agree or disagree with how safe they feel performing the functions on a laptop/desktop and then on a smartphone. The respondents are asked to take into account the safety of their personal information when answering. I used a 5-scale Likert scale. The questions here get to the heart of my research question, is there a difference in perceived safety between a laptop/desktop and a smartphone. I am going to breakdown this question with many smaller questions. I want to first see if there is an overall difference in perceived security combining all functions together. I then want to look at the different demographic areas and see if there is an overall difference between them. To just name a few of the examples, I will look at sex versus overall perceived security, victim history versus overall perceived security and risk aversion/tolerance versus overall perceived security. After that is competed I want to break down the differences in perceived security for each of the six functions.

The final section deals with any measures students are using to mitigate security risks on their devices. In this section, the survey asked respondents rate their agreement about how often they use six different security technologies on both laptop/desktops and smartphones. The six technologies are password protection, remote locate lock and wipe, back-up data, apply system updates, VPN for Wi-Fi hotspots, and anti-virus software. Again a 5-point Likert scale was used to measure the response. From this information I am looking to see if there is an overall difference in security and then to break it down between the six technologies. Just like the last section, I will break down this response between the different demographic groups.

The survey had many Likert scales, so I had to transform the data for comparisons. The questions that contained Likert scales had the answers rated from 1 to 5, 1 for strongly agree and 5 for strongly disagree. There were three questions that dealt with computer knowledge. These three questions were averaged for each respondent to compute overall computer knowledge. Scores less than 2 were categorized as ‘High’ and scores 2 to 3 were categorized as ‘Moderate’. There were no scores that averaged more than 3. The next three questions dealt with computer risk/tolerance. These three scores were also averaged for each respondent to compute an overall computer risk ideal. Scores less than 2.5 were categorized as ‘Tolerant’, scores between 2.5 and 3.5 were ‘Neutral’ and scores more than 3.5 were ‘Averse’.

In order to analyze and test all of these items, I will be using hypothesis testing with t-tests, confidence intervals and analysis of variance. The statistical software I will be using to run these test is SAS (Statistical Analysis System). For analyses with only two options, like gender, and one response variable, I will use a 2-sample t-test. If there are more than two options, like school year, I will use a one-way analysis of variance (ANOVA). In both cases, a 95% confidence interval will be created and boxplots will be shown.

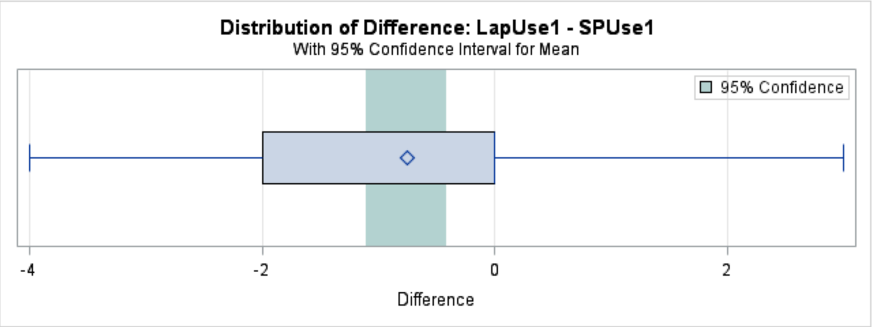
Chapter 5

Results

Differences in Functions

The first research question dealt with the difference in the use of six functions on a laptop/desktop versus a smartphone. These values come the responses of questions 9 and 10 (Appendix A). The SAS code and output of the t-tests can be found in Appendix C. The boxplots are shown. Online banking was the first function examined. The average score for online banking on laptops/desktops was 1.92 and the average for smartphones was 2.68. This leads to an average difference of -0.76.

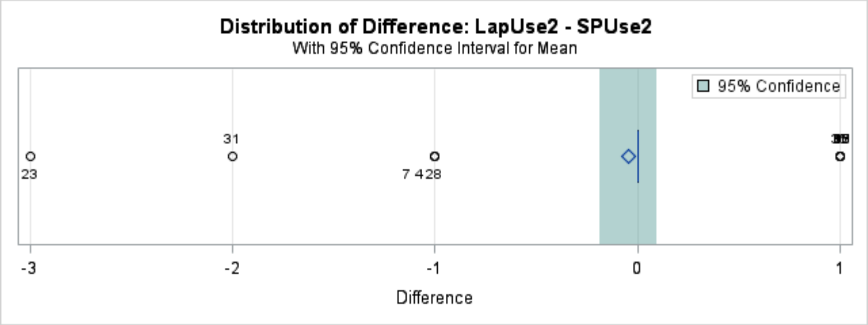
Figure 5-1 Online Banking Use Difference



Using a t-test we found a p-value of less than .0001 and the difference was significant. Figure 5-1 also shows that the 95% confidence interval does not include the value 0. Students perform online banking more often on a laptop/desktop than on a smartphone.

The second function is frequency the respondent uses social networking. The average score for laptops/desktops was 1.27 and 1.32 for smartphones. 1.32 was the lowest rating for smartphone functions, meaning it was used the most often. The difference in the two averages is -0.05.

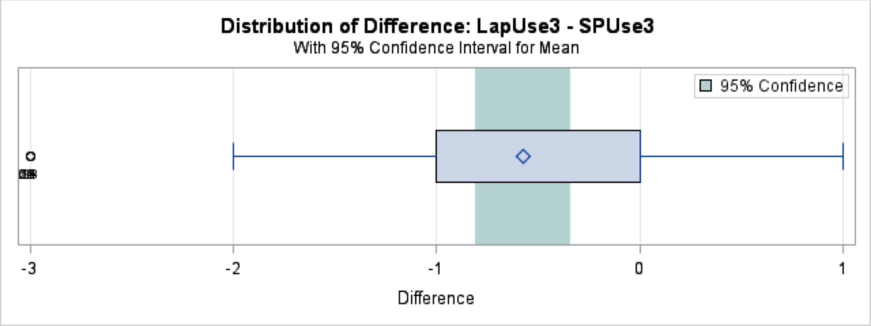
Figure 5-2 Social Networking Use Difference



After running the t-test, the difference in social networking on laptops/desktops and smartphones shows no significant difference with a p-value of .52. The value 0 is found in the 95% confidence interval (shown in Figure 5-2) making the difference not significant as well.

Internet surfing usage was considered next. Laptops/desktops had an average score of 1.30 whereas smartphones had an average score of 1.88. The average difference between the two was -0.58.

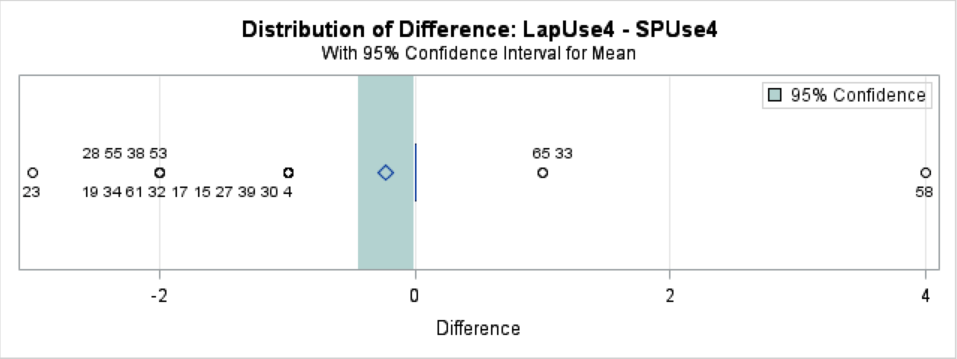
Figure 5-3 Internet Surfing Use Difference



After looking at the t-test, which resulted in a p-value less than .0001, there was a significant difference. Figure 5-3 proves this by showing that 0 is not within the 95% confidence interval.

Email had the lowest score among laptop/desktop users with 1.24. This means that on average email was used the most often of all the functions on laptops/desktops. The average score for email use on a smartphone was 1.47 leading to a difference of -0.23.

Figure 5-4 Email Use Difference



Again the t-test, with a p-value of .04, and 95% confidence interval (Figure 5-4) show that the difference is significant. Email is used more often on laptops then smartphones.

The next function that was analyzed is online gaming. The average for laptop/desktops is 3.48 and the average for smartphones is 3.23. This leads to an average difference of 0.25. The score of 3.48 was the lowest for laptop/desktop users, meaning it was used the least often.

Figure 5-5 Online Gaming Use Difference

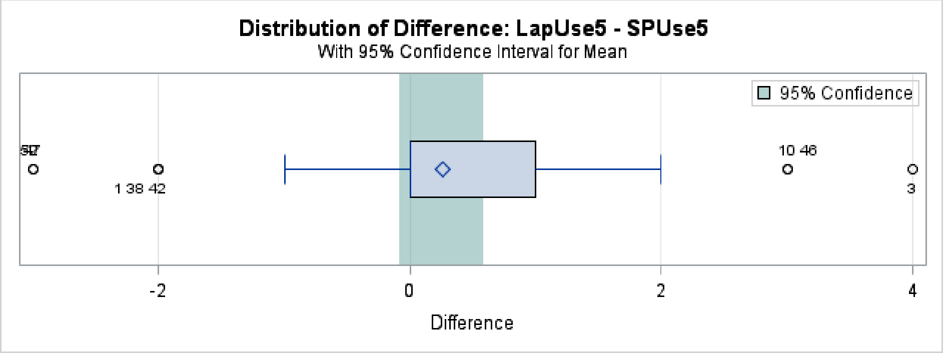
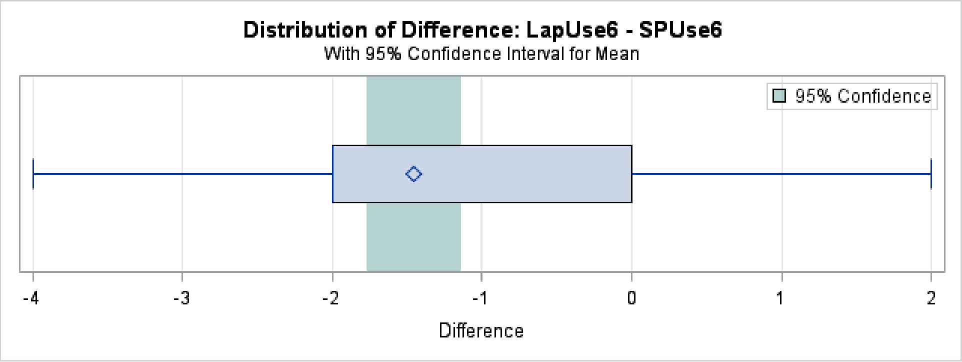


Figure 5-5 shows that 0 is inside the 95% confidence interval leading to the difference not being significant. The t-test also proves that the difference is not significant by resulting in a p-value of .13.

The final function the survey covered was e-commerce (shopping). The average laptop/desktop score was 2.02 and the average smartphone score was 3.47. This resulted in a difference of -1.45, the greatest of all the functions studied.

Figure 5-6 E-Commerce Use Difference



It is clear that the 95% confidence interval does not include 0. The p-value of the t-test is less than .0001. Both of these facts lead to a significant difference, meaning students shop on their laptop/desktop more than their smartphones.

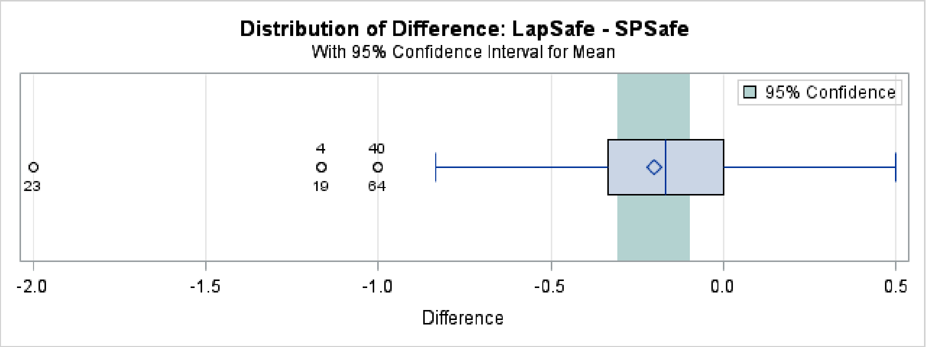
In summary, I found significant differences in the uses of online banking, Internet surfing, email and e-commerce. The differences in all of these functions were negative, leading to a result that uses performed these four functions more frequently on a laptop/desktop than on a smartphone. There are several possible reasons why I found differences among these functions. One could be the quality of user-interface. The size of the screen on a laptop/desktop and the website allow user to see and do more at one time. Surfing the Internet and shopping online may be more effective and time efficient on a laptop/desktop than a smartphone. The difference in email use is a clear example of the quality of user interface. Many people prefer typing emails on a full keyboard and not the touch keyboard usually found on smartphones. If the function was just limited to checking email and not responding, the results could be different. Another reason for the difference could be perceived safety. On laptops/desktops, users may have installed more security options like anti-virus and malware to secure themselves. Online banking and e-commerce require the user to input personal information, credit card numbers and financial account numbers. A user would give up this information more often in a place they feel secure. In order to study this reason more, differences in safety will be studied.

Differences in Safety

This section focuses on the main research question of perceived security. The response variable I will be using is the difference of the average scores of question 11 and 12 (Appendix A). At first I will look at the overall average score across all six functions. I will break down the overall differences further by comparing it with the demographic information. Finally, each of the six functions will be compared individually.

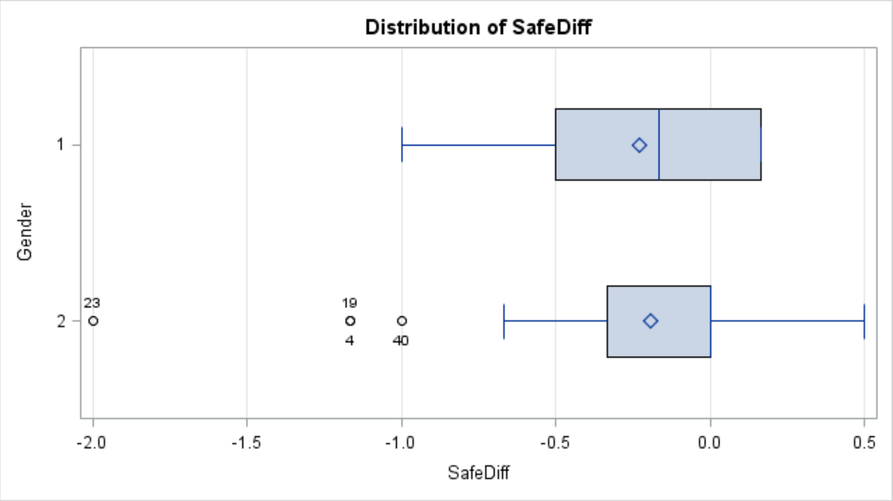
The overall difference will be computed by taking each respondent’s average across the six functions. The overall average for feeling safe on a laptop/desktop was 2.02 and 2.22 for a smartphone. After computing the t-test and looking at the confidence interval, we can see that there is a significant difference between the two. The p-value was .0003 and the confidence interval is shown below (Figure 5-7).

Figure 5-7- Overall Security Differences



The next item I wanted to examine was any difference between men and women. Although only 19 males responded versus 47 females, it was still important to see if there was a difference. The mean difference for men was -0.23 and -0.19 for women.

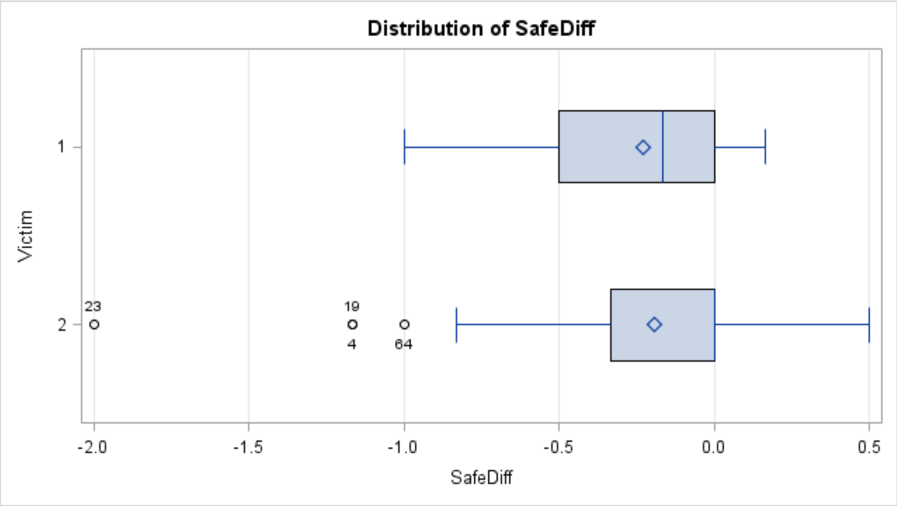
Figure 5-8- Gender Differences



After performing a t-test analyzing male (gender 1) and female (gender 2) no significant difference was found (Appendix C). The lack of significance is also visible in figure 5-8 (above).

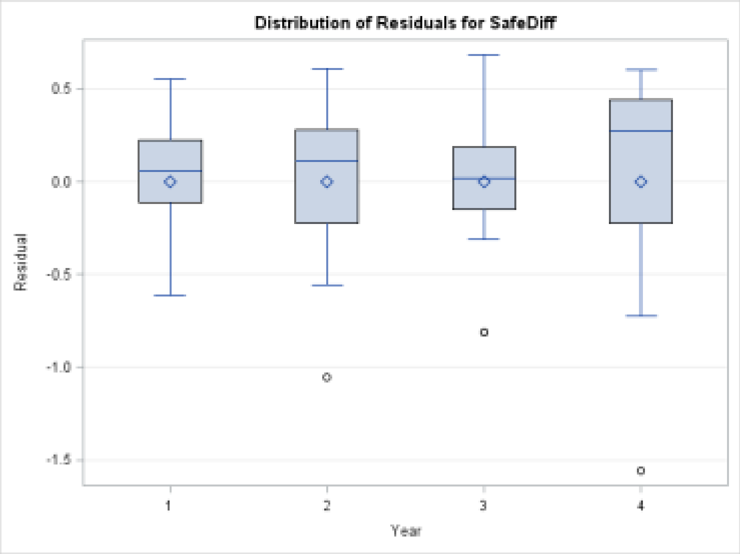
Another item of interest was whether the respondent had a history of a computer security incident. I wanted to look at if being a victim of an attack had an impact of the difference between laptop and smartphone security. Answering yes to being a victim was coded as “1” and no was coded as “2”. Again, there was no significant difference found after performing the t-test. The figure 5-9 below also illustrates this point.

Figure 5-9 Differences in Victim History



The next demographic question involved the respondents year in college. The respondents were classified into four different groups: freshman (coded as 1), sophomore (2), junior (3) and senior (4). A one-way ANOVA was used to measure any differences. The test resulted in no significant difference found between any of the groups and the boxplot below shows very similar results (Figure 10).

Figure 5-10 Differences in School Year



In addition to the demographic questions above, the respondents were asked questions regarding their computer knowledge and their computer risk behavior. Question 7 (Appendix A) involved computer knowledge and respondents were broken into two groups, high and moderate based on their answers. Based on answers to question 8 (Appendix A), respondents were broken in to three groups: averse, neutral and tolerant. One-way ANOVA tests and boxplots were constructed and analyzed to see if there was any difference in safety perceptions. The tests (Appendix C) and the boxplots (Figures 5-11 and 5-12) did not display any significant results.

Figure 5-11 Difference in Computer Knowledge

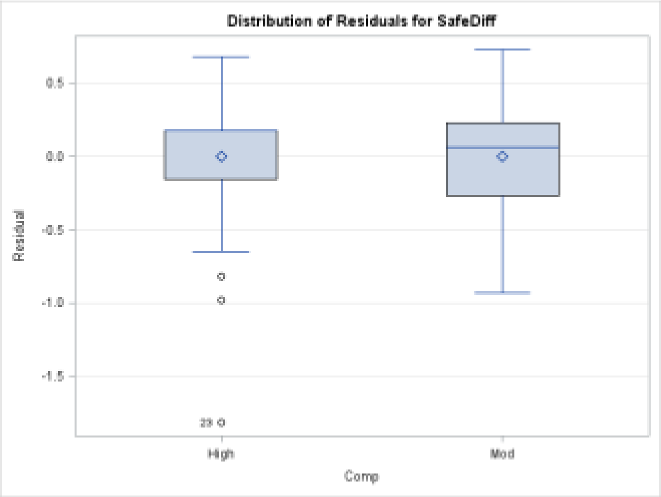
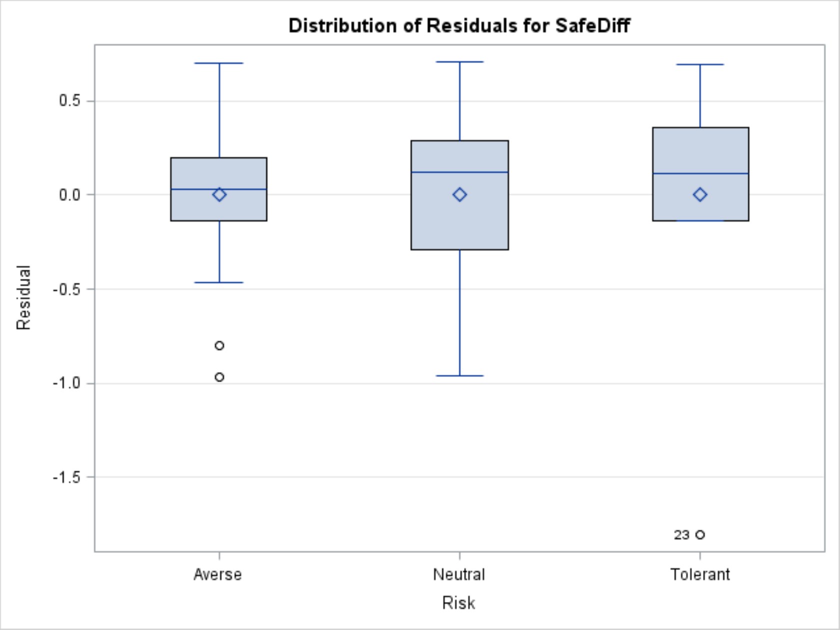


Figure 5-12 Differences in Risk Behaviors



The next step in breaking down the safety data is to look at each function individually. This is similar to what how the use questions were broken down. This will show whether there is a difference in the perceived safety of using a laptop/desktop versus a smartphone in the six functions of online banking, social networking, Internet surfing, email, online gaming and e-commerce. In order to analyze the data, t-tests were used on each of the functions. In total there were two functions that had a significant difference: online banking and e-commerce. Both of these differences had p-values less than .0001 and were very significant. In both cases users felt safer on their laptop/desktop than on their smartphone. In these significant functions the user shares a lot of their important personal information. One of the reasons people feel safer on laptop/desktops could be that they use the device more often at home with a trusted network versus a public network. It could also be that there are more safeguards on the website versus the mobile banking application. All of the tests can be found in Appendix C and the resulting boxplots are found below (Figures 5-13 to 5-18).

Figure 5-13 Online Gaming Safety Differences

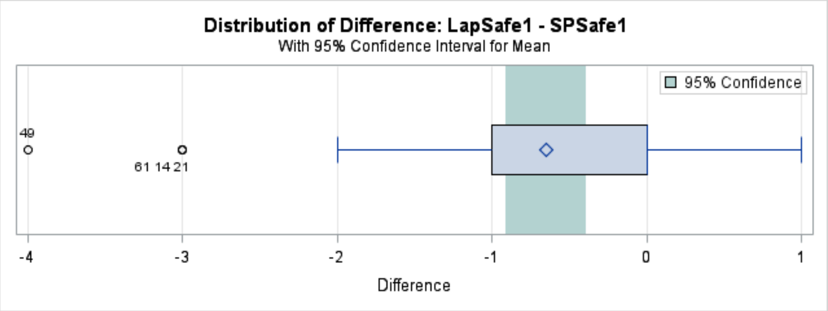


Figure 5-14 Social Networking Safety Differences

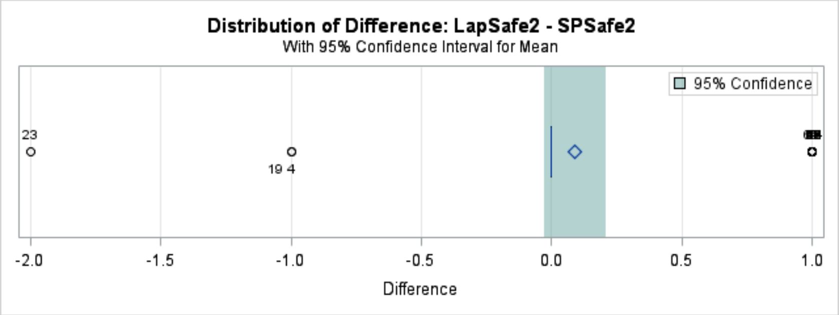


Figure 5-15 Internet Surfing Safety Differences

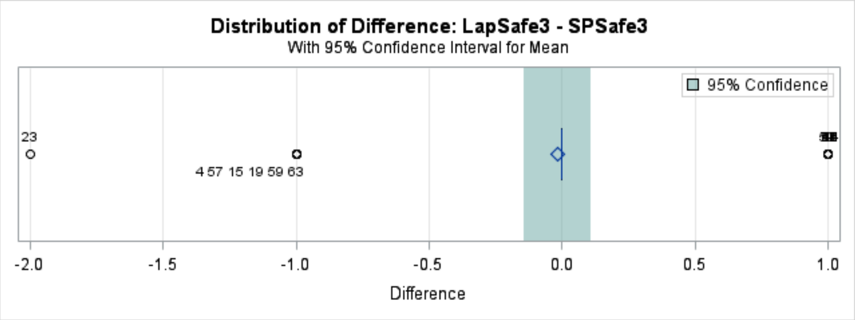


Figure 5-16 Email Safety Differences

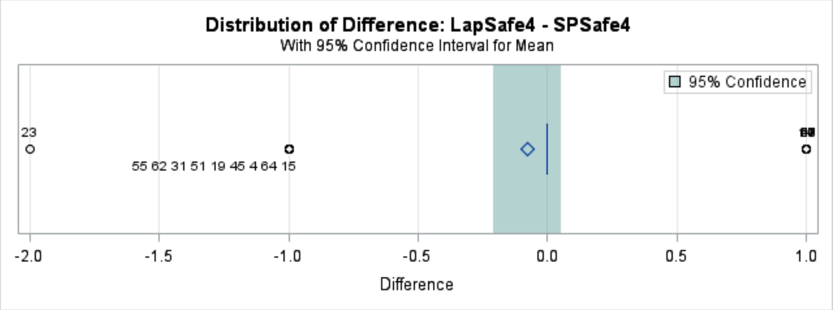


Figure 5-17 Online Gaming Safety Differences

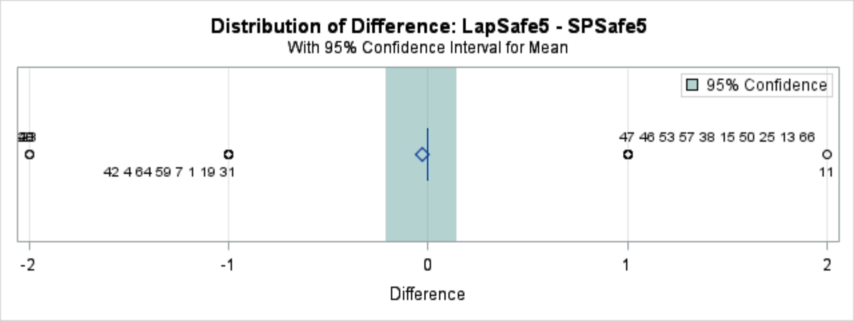
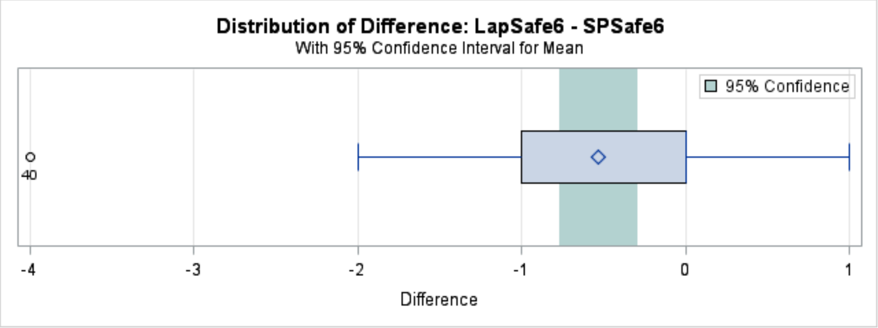


Figure 5-18 E-Commerce Safety Differences

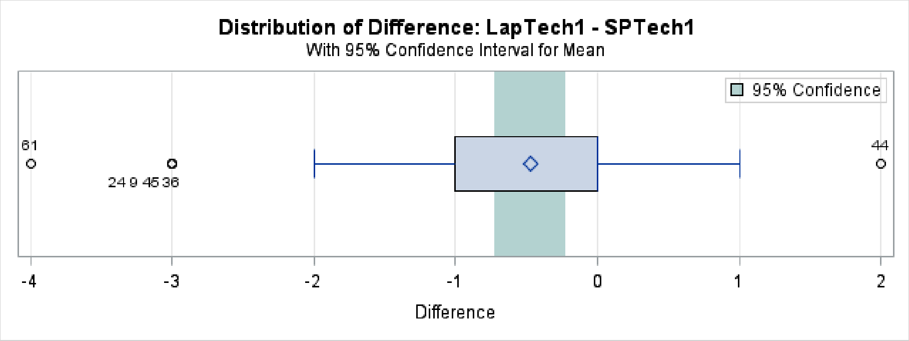


Differences in Security Options

So far the perceived safety of laptop and smartphones has been measured. Next the actual security devices in place on each device will be examined. The survey measured the use of six common security devices: password protection, remote locate/lock and wipe, data back-up, system updates, VPN for Wi-Fi Hotspots, and Anti-virus software. The respondents were asked how often they used each feature on a laptop/desktop and then on a smartphone. The same 5-point Likert scale was used to measure the responses.

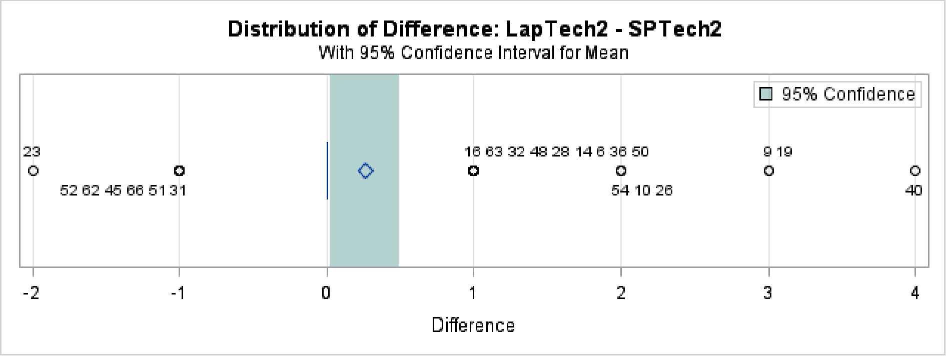
The first device analyzed was password protection. This simply meant enabling any type of password in order to logon or access the device. The average score for laptops/desktops was 1.44 and was 1.91 for smartphones. Using a t-test to analyze this difference, a p-value of .0004 was found. The difference is significant according to the test and the confidence interval constructed below (Figure 5-19). Students use passwords more often on their laptops than on their smartphones. I was surprised to see a difference here due to the popularity of passwords on both devices. The difference could result in the other uses for laptop/desktops versus smartphones. Laptop/desktops have large storage capacity. Many important documents, pictures and data are kept on these devices, whereas most of the memory on smartphones is used for applications and music. Something interesting to look at in the future would be to see if the strength of passwords between the devices is different.

Figure 5-19 Password Protection Differences



The next device asked about was a remote location, lock and wipe application. The point of this application is to access the laptop or smartphone from far away. For example in case the smartphone is stolen, the application can erase all of the data from the phone. This keeps the owner's sensitive and personal information safe. The average score for laptops/desktops was 3.14 and 2.88 for smartphones. The confidence interval below (Figure 5-20) shows a slight positive significant difference and a t-test confirms this. This application is more often used by students on smartphones than laptops. The result makes sense considering this application is more apparent on smartphones.

Figure 5-20 Remote Locate, Lock and Wipe Differences



The next three devices looked at were data back-up, system updates, VPN for Wi-Fi Hotspots. Backing-up data is important security item in case a system is infected and needs to be re-installed. System updates install fixes to newly found vulnerabilities and is an important aspect to security. VPN or virtual private network creates a safe connection for Wi-Fi use when the user is in public places. This safety feature keeps intrudes from stealing packets and information on a public network. The analysis of these questions leads to no significant results. The confidence intervals can be found below and the t-tests in Appendix C.

Figure 5-21 Back-Up Data Differences

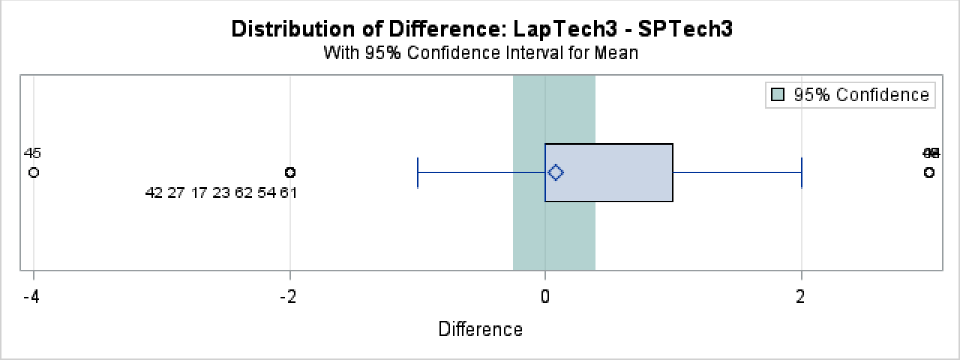


Figure 5-22 System Update Differences

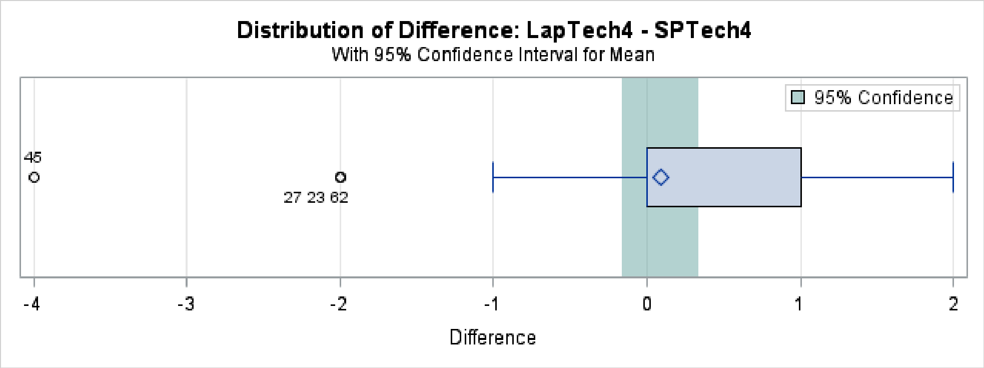
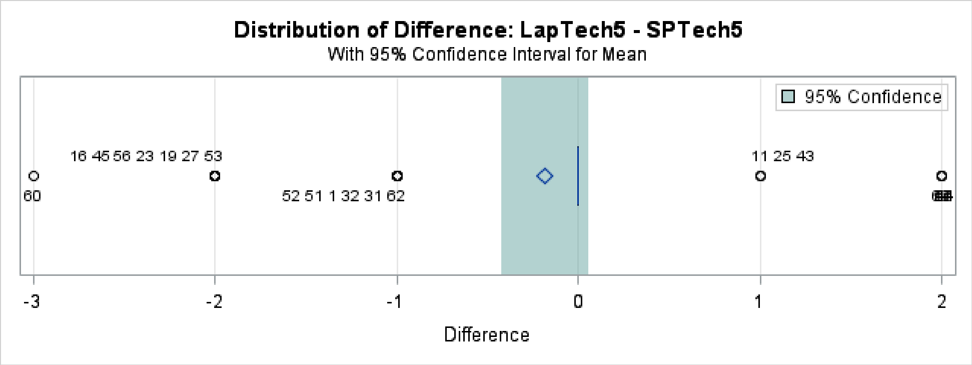
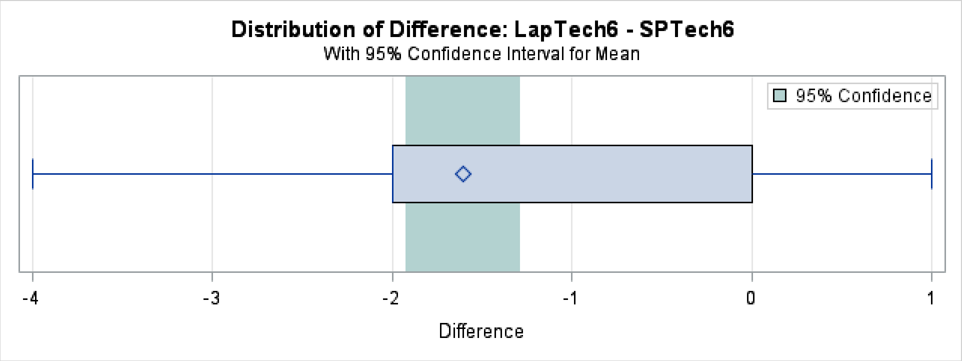


Figure 5-23 VPN for Wi-Fi Hotspots



The final security device examined was the use of anti-virus software. After computing a t-test and a confidence interval, there was a large significant difference. Anti-virus software was used a lot more on laptops/desktops than smartphones. This is to be expected as the software is very common on laptop/desktops and not so much on smartphones.

Figure 5-24 Anti-virus Software Differences



Chapter 6

Summary of Findings and Conclusion

The main research question this paper looked at was whether there is a difference in the perceived safety of laptop/desktop versus smartphones. When the overall differences were compared, there was a significant difference. Upon further investigation, perceived safety was broken down by application. Of the six studied applications, online banking and e-commerce had significant differences. In both cases the respondents felt safer using a laptop/desktop than a smartphone. Many companies are offering options for mobile applications to transfer money, read checks, and take in credit card information. They spend money and time developing and maintain these applications. From the study, we have seen that students use online banking and e-commerce more frequently on laptops than smartphones. One of the significant security options was the difference in anti-virus use. Respondents may use and feel safer on laptop/desktops because they use anti-virus software more often. Online banking and e-commerce require the sharing of important personal information. The higher use of anti-virus on laptop/desktops could be one of the leading reasons the respondents used and felt safer on them. As smartphone use gets more popular, it will be important to do more research into why students feel less comfortable on them and use them less. If companies really want their banking applications to be successful, they may want to educate their customers on the safety of the application.

Another aspect I wanted to analyze was whether a respondent’s risk behavior had any impact on differences. In order to measure whether someone was risk tolerant, risk neutral or risk adverse, I created three questions whose scores I averaged. This could be due to the questions not measuring risk well enough. Similarly, I wanted to look at whether being a victim of a computer security incident had any effect on differences. I coded the answer as a binary yes or no and didn’t get any significant results. I did not on measure it on a scale of how bad the incident was. Maybe there are significant results when I look at severe incidents versus never having had an incident.

One step in increasing the use and perceived safety of smartphone security would be to educate students. The study showed that password protection was the most popular security option. Another positive coming from the study showed a high rate of applying system updates especially on smartphones. One security function that needs to be taught and utilized more is virtual private network (VPN) usage. In both laptops and smartphones the scores were about in the middle for how often respondents used them. VPNs are a great way to send secure data through wireless networks. People of all ages, not just students should be made more aware of this option.

No study is perfect and there are many problems to consider. The following options could be considered in future studies. A variable that could impact validity is the type of application use. There are many different applications to perform the same action across devices. In some cases the application on a laptop may be much easier to use than the same type of application on a smartphone. The survey conducted included questions about how comfortable respondents are performing certain actions on each device. The user’s preference of device could come from the ease of application not necessarily the security of the device. In future research, the survey could emphasize that the respondent should focus on the security aspect of each application. Future research could also choose applications that have a very similar if not identical user interface.

A main threat to external validity is the difference in the volunteers and the target average population. I used a convenience sample, which means I asked people to volunteer to fill out my survey. The people who agree to fill out a survey on laptop and mobile security may have different characteristics. People who feel comfortable enough to fill out a survey on security may have more knowledge on security than the average college student. This could lead to skewed data where a certain group is not being represented. Future studies could address this limitation through the use of a stratified random sample. Stratified random sampling involves breaking the population up into different groups and then sampling from there. Three different majors of different technology levels will be selected and individuals will be sampled from there.

There are two big areas of research that can expand on this paper. While this study is focusing on college students and their level of perceived security, a great area of future research would be in the business/ professional world. Businesses handle so much private and personal data and information that it is very important to keep up with security. There is also a lot of travel within certain industries and smartphones are being used more and more to connect to company's secure networks. If data was found to prove there is also a difference in perceived security. Businesses can add or increase smartphone education into their training programs with new and current employees. The other area of future research is in tablet computers. Devices such as the iPad and the Samsung Galaxy Tab are gaining vast popularity. Perceptions of security on tablets can added to this research and compared to perceptions of security on smartphones and laptops as these devices perform similar functions.

Appendix A

Research Survey

Perceptions of Smartphone Security

Q1 Informed Consent

Conducted as part of the undergraduate thesis requirement for the Schreyer Honors College, The Pennsylvania State University

Please read this consent document before you decide to participate in this study.

Purpose of the research study:

This study is designed to determine the perception of Smartphone vs. Laptop security and what actions people are more comfortable using on each device.

What you will be asked to do in this study:

You will be asked to answer some multiple choice questions about your Smartphone and Laptop usage and technology preferences.

Time required: 15-20 minutes

Risks:

There are no anticipated discomforts in completing this survey. You can withdraw from participation at any stage of the survey.

Compensation and Benefit:

The results will be used to benefit undergraduate research at Penn State University in the Schreyer Honors College.

Confidentiality:

Your identity will be kept confidential as required by law. Your name will never appear in any related report. No identifying information will be gathered. All responses are anonymous. No guarantees can be made regarding interception of data sent via the Internet by any third parties.

Voluntary Participation:

Your participation in this study is completely voluntary. There is no penalty for not participating.

Right to withdraw from the study: You may withdraw from the study at any time without consequence.

The IRB title and number for this survey is IRB 44862 Perceptions of Smartphone Security.

Point of contact for questions related to the study:

Kevin Laubscher, kal5286@psu.edu

Agreement:

I have read the above information. Clicking on the “Next” button below indicates that I voluntarily agree to participate in the survey.

Q2 Gender:

Male (1)

❍ Female (2)

Q3 What year in college are you?

❍ Freshman (1)
❍ Sophomore (2)
❍ Junior (3)
❍ Senior (4)

Q4 Do you own a Smartphone?

❍ Yes (1)
❍ No (2)

Q5 Do you own a Laptop or Desktop Computer?

❍ Yes (1)
❍ No (2)

Q6 Have you ever been a victim of a computer security incident?

❍ Yes (1)
❍ No (2)

Q7 To what extent do you agree or disagree with the following statements about your technical knowledge:

	Strongly Agree (1)	Agree (2)	Neither Agree nor Disagree (3)	Disagree (4)	Strongly Disagree (5)
I am comfortable installing software on my computer. (1)	❍	❍	❍	❍	❍
I am comfortable using word processing and presentation software. (2)	❍	❍	❍	❍	❍
I am comfortable downloading applications and files to my Smartphone. (3)	❍	❍	❍	❍	❍

Q8 To what extent do you agree or disagree with the following statements about computer risk:

	Strongly Agree (1)	Agree (2)	Neither Agree nor Disagree (3)	Disagree (4)	Strongly Disagree (5)
I feel comfortable downloading files of unknown origin (songs, movies, documents etc.). (1)	❍	❍	❍	❍	❍
I feel comfortable sharing personal information online (name, birthday, current residence etc.). (2)	❍	❍	❍	❍	❍
I feel comfortable joining networks/communities with people I don't know. (3)	❍	❍	❍	❍	❍

Q9 To what extend do you agree or disagree with the following statements. I often perform the following actions while using a Laptop or Desktop.

	Strongly Agree (1)	Agree (2)	Neither Agree nor Disagree (3)	Disagree (4)	Strongly Disagree (5)
Online Banking (1)	❍	❍	❍	❍	❍
Social Networking (2)	❍	❍	❍	❍	❍
Internet Surfing (3)	❍	❍	❍	❍	❍
Email (4)	❍	❍	❍	❍	❍
Online Gaming (5)	❍	❍	❍	❍	❍
E-Commerce (Shopping) (6)	❍	❍	❍	❍	❍

Q10 To what extend do you agree or disagree with the following statements. I often perform the following actions while using a Smartphone.

	Strongly Agree (1)	Agree (2)	Neither Agree nor Disagree (3)	Disagree (4)	Strongly Disagree (5)
Online Banking (1)	❍	❍	❍	❍	❍
Social Networking (2)	❍	❍	❍	❍	❍
Internet Surfing (3)	❍	❍	❍	❍	❍
Email (4)	❍	❍	❍	❍	❍
Online Gaming (5)	❍	❍	❍	❍	❍
E-Commerce (Shopping) (6)	❍	❍	❍	❍	❍

Q11 To what extent to you agree or disagree with the following statement: I feel safe performing the below actions/tasks while using a Laptop or Desktop. Safety includes the safety of your personal information.

	Strongly Agree (1)	Agree (2)	Neither Agree nor Disagree (3)	Disagree (4)	Strongly Disagree (5)
Online Banking (1)	○	○	○	○	○
Social Networking (2)	○	○	○	○	○
Internet Surfing (3)	○	○	○	○	○
Email (4)	○	○	○	○	○
Online Gaming (5)	○	○	○	○	○
E-Commerce (Shopping) (6)	○	○	○	○	○

Q12 To what extent to you agree or disagree with the following statement: I feel safe performing the below actions/tasks while using a Smartphone. Safety includes the safety of your personal information.

	Strongly Agree (1)	Agree (2)	Neither Agree nor Disagree (3)	Disagree (4)	Strongly Disagree (5)
On-line Banking (1)	○	○	○	○	○
Social Networking (2)	○	○	○	○	○
Internet Surfing (3)	○	○	○	○	○
Email (4)	○	○	○	○	○
On-line Gaming (5)	○	○	○	○	○
E-Commerce (Shopping) (6)	○	○	○	○	○

Q13 To what extent do you agree or disagree. On my Laptop or Desktop, I often use the following security options:

	Strongly Agree (1)	Agree (2)	Neither Agree nor Disagree (3)	Disagree (4)	Strongly Disagree (5)
Password Protection (1)	❍	❍	❍	❍	❍
Remote Locate, Lock and Wipe (2)	❍	❍	❍	❍	❍
Back-Up Data (3)	❍	❍	❍	❍	❍
Apply System Updates (4)	❍	❍	❍	❍	❍
VPN for Wi-Fi Hotspots (5)	❍	❍	❍	❍	❍
Anti-Virus Software (6)	❍	❍	❍	❍	❍

Q14 To what extent do you agree or disagree. On my Smartphone, I often use the following security options:

	Strongly Agree (1)	Agree (2)	Neither Agree nor Disagree (3)	Disagree (4)	Strongly Disagree (5)
Password Protection (1)	❍	❍	❍	❍	❍
Remote Locate, Lock and Wipe (2)	❍	❍	❍	❍	❍
Back-Up Data (3)	❍	❍	❍	❍	❍
Apply System Updates (4)	❍	❍	❍	❍	❍
VPN for Wi-Fi Hotspots (5)	❍	❍	❍	❍	❍
Anti-Virus Software (6)	❍	❍	❍	❍	❍

Appendix B

Table of Variables in SAS

Variable Name	**Explanation of Variable** (question numbers refer to survey in Appendix A)	**Variable Options**
Consent	Whether the respondent agreed to the consent page	1=Yes, 2=No
Gender	Gender of the respondent	1=Male, 2=Female
Year	Year of the respondent in school	1=Freshman, 2=Sophomore, 3=Junior, 4=Senior
Smartphon	Whether or not the respondent has a smartphone	1=Yes, 2=No
Laptop	Whether or not the respondent has a laptop or a desktop	1=Yes, 2=No
Victim	Whether or not the respondent has ever been a victim of a computer security incident	1=Yes, 2=No
Comp	The classification of the respondent's computer knowledge	Mod, High
Risk	The classification of the respondent's computer risk	Tolerant, Neutral, Averse
LapUse1 / SPUse1	Rating of how often respondent uses each device for online banking	1=Strongly Agree … 5=Strongly Disagree
LapUse2 / SPUse2	Rating of how often respondent uses each device for social networking	1=Strongly Agree … 5=Strongly Disagree
LapUse3 / SPUse3	Rating of how often respondent uses each device for Internet surfing	1=Strongly Agree … 5=Strongly Disagree
LapUse4 / SPUse4	Rating of how often respondent uses each device for email	1=Strongly Agree … 5=Strongly Disagree
LapUse5 / SPUse5	Rating of how often respondent uses each device for online gaming	1=Strongly Agree … 5=Strongly Disagree
LapUse6 / SPUse6	Rating of how often respondent uses each device for e-commerce	1=Strongly Agree … 5=Strongly Disagree
LapSafe1 / SPSafe1	Rating of how safe the respondent feels while using each device for online banking	1=Strongly Agree … 5=Strongly Disagree
LapSafe2 / SPSafe2	Rating of how safe the respondent feels while using each device for social networking	1=Strongly Agree … 5=Strongly Disagree
LapSafe3 / SPSafe3	Rating of how safe the respondent feels while using each device for Internet surfing	1=Strongly Agree … 5=Strongly Disagree

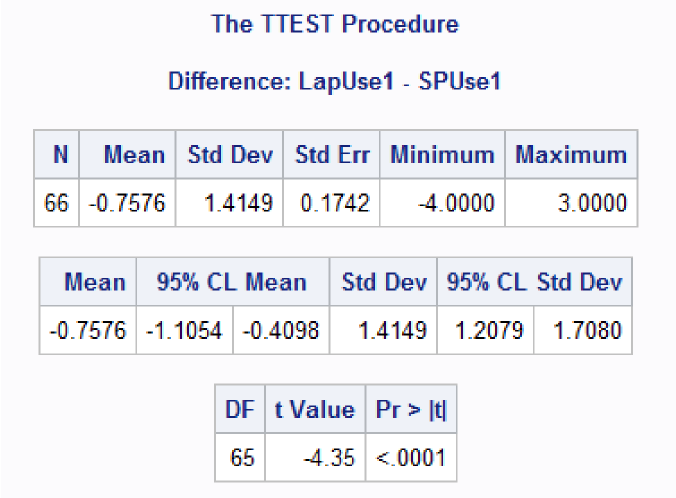
LapSafe4 / SPSafe4	Rating of how safe the respondent feels while using each device for email	1=Strongly Agree … 5=Strongly Disagree
LapSafe5 / SPSafe5	Rating of how safe the respondent feels while using each device for online gaming	1=Strongly Agree … 5=Strongly Disagree
LapSafe6 / SPSafe6	Rating of how safe the respondent feels while using each device for e-commerce	1=Strongly Agree … 5=Strongly Disagree
LapSafe / SPSafe	Average rating of how safe the respondent feels while performing all six actions on each device	1 - 5
LapTech1 / SPTech1	Rating of how often the respondent uses password protection on each device	1=Strongly Agree … 5=Strongly Disagree
LapTech2 / SPTech2	Rating of how often the respondent uses remote locate, wipe and lock on each device	1=Strongly Agree … 5=Strongly Disagree
LapTech3 / SPTech3	Rating of how often the respondent backs-up data on each device	1=Strongly Agree … 5=Strongly Disagree
LapTech4 / SPTech4	Rating of how often the respondent applies system updates on each device	1=Strongly Agree … 5=Strongly Disagree
LapTech5 / SPTech5	Rating of how often the respondent uses VPN for Wi-Fi hotspots on each device	1=Strongly Agree … 5=Strongly Disagree
LapTech6 / SPTech6	Rating of how often the respondent uses anti-virus software on each device	1=Strongly Agree … 5=Strongly Disagree
LapTech / SPTech	Average rating of how often the respondent uses the six security options on each device	1 - 5

Appendix C

SAS Code and Output

Differences in Functions

Online Banking:



The TTEST Procedure

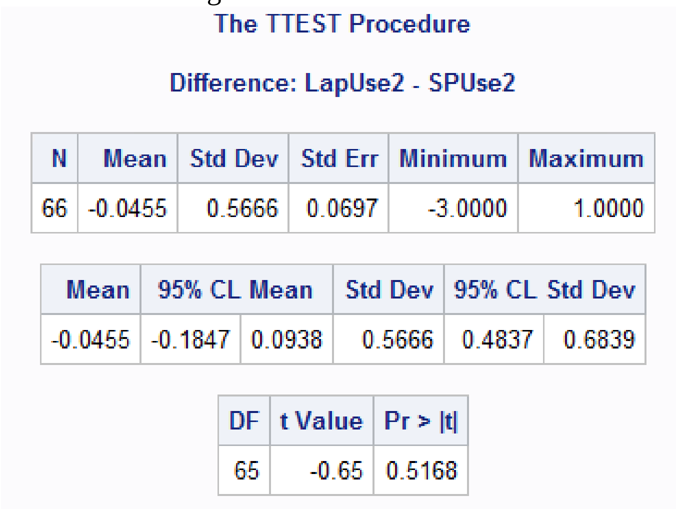
Difference: LapUse1 - SPUse1

N	Mean	Std Dev	Std Err	Minimum	Maximum
66	-0.7576	1.4149	0.1742	-4.0000	3.0000

Mean	95% CL Mean		Std Dev	95% CL Std Dev	
-0.7576	-1.1054	-0.4098	1.4149	1.2079	1.7080

DF	t Value	Pr > |t|
65	-4.35	<.0001

Social Networking:



The TTEST Procedure

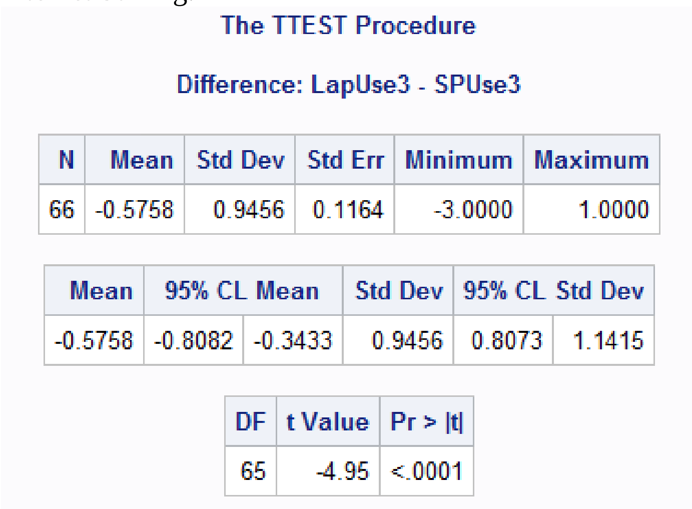
Difference: LapUse2 - SPUse2

N	Mean	Std Dev	Std Err	Minimum	Maximum
66	-0.0455	0.5666	0.0697	-3.0000	1.0000

Mean	95% CL Mean		Std Dev	95% CL Std Dev	
-0.0455	-0.1847	0.0938	0.5666	0.4837	0.6839

DF	t Value	Pr > |t|
65	-0.65	0.5168

Internet Surfing:



The TTEST Procedure

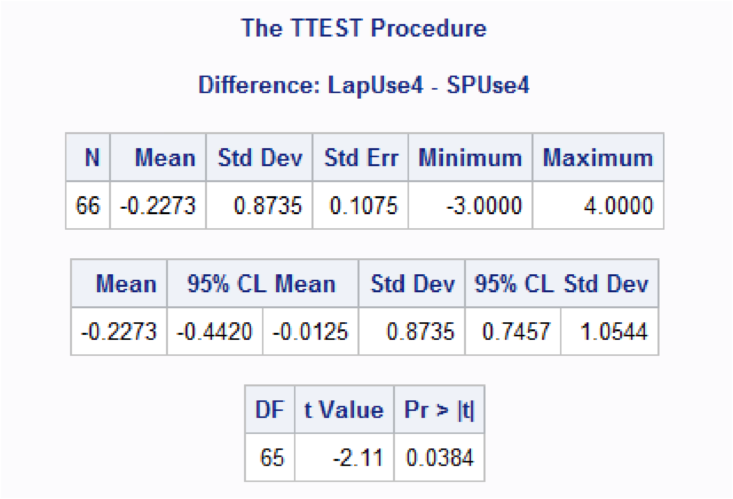
Difference: LapUse3 - SPUse3

N	Mean	Std Dev	Std Err	Minimum	Maximum
66	-0.5758	0.9456	0.1164	-3.0000	1.0000

Mean	95% CL Mean		Std Dev	95% CL Std Dev	
-0.5758	-0.8082	-0.3433	0.9456	0.8073	1.1415

DF	t Value	Pr > |t|
65	-4.95	<.0001

Email:



The TTEST Procedure

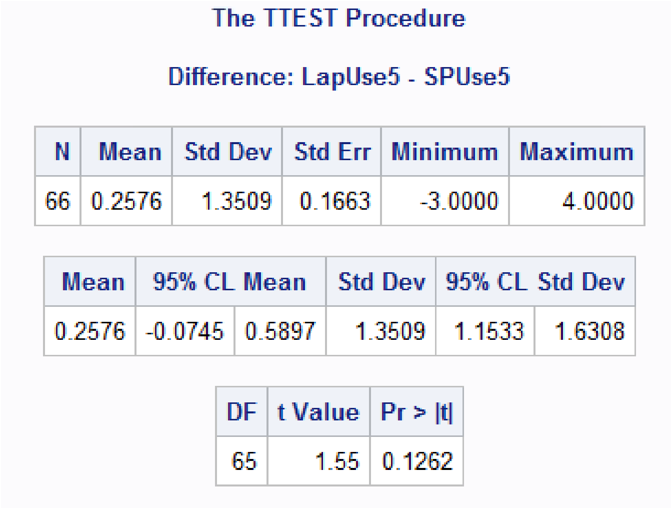
Difference: LapUse4 - SPUse4

N	Mean	Std Dev	Std Err	Minimum	Maximum
66	-0.2273	0.8735	0.1075	-3.0000	4.0000

Mean	95% CL Mean		Std Dev	95% CL Std Dev	
-0.2273	-0.4420	-0.0125	0.8735	0.7457	1.0544

DF	t Value	Pr > |t|
65	-2.11	0.0384

Online Gaming:



The TTEST Procedure

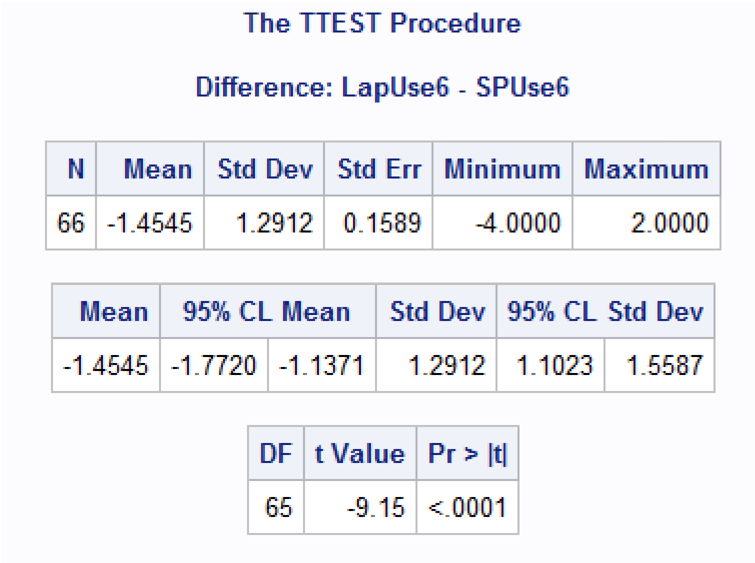
Difference: LapUse5 - SPUse5

N	Mean	Std Dev	Std Err	Minimum	Maximum
66	0.2576	1.3509	0.1663	-3.0000	4.0000

Mean	95% CL Mean		Std Dev	95% CL Std Dev	
0.2576	-0.0745	0.5897	1.3509	1.1533	1.6308

DF	t Value	Pr > |t|
65	1.55	0.1262

E-Commerce:



The TTEST Procedure

Difference: LapUse6 - SPUse6

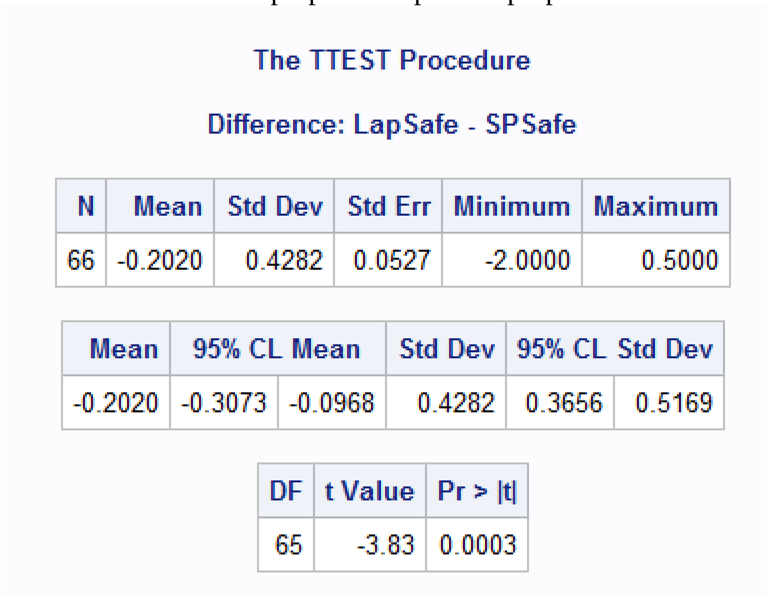
N	Mean	Std Dev	Std Err	Minimum	Maximum
66	-1.4545	1.2912	0.1589	-4.0000	2.0000

Mean	95% CL Mean		Std Dev	95% CL Std Dev	
-1.4545	-1.7720	-1.1371	1.2912	1.1023	1.5587

DF	t Value	Pr > |t|
65	-9.15	<.0001

Differences in Safety

Overall Differences Laptop/Desktop vs. Laptop:



The TTEST Procedure

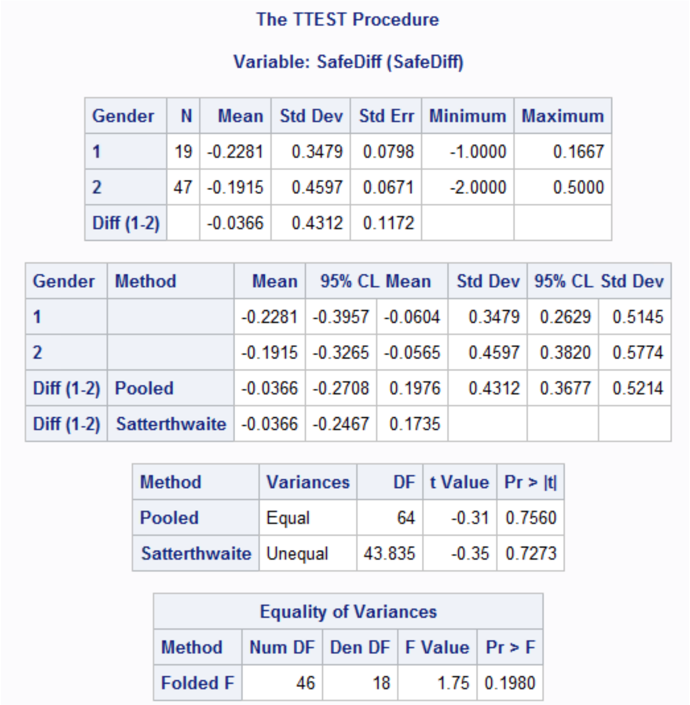
Difference: LapSafe - SPSafe

N	Mean	Std Dev	Std Err	Minimum	Maximum
66	-0.2020	0.4282	0.0527	-2.0000	0.5000

Mean	95% CL Mean		Std Dev	95% CL Std Dev	
-0.2020	-0.3073	-0.0968	0.4282	0.3656	0.5169

DF	t Value	Pr > |t|
65	-3.83	0.0003

Differences in Gender:



The TTEST Procedure

Variable: SafeDiff (SafeDiff)

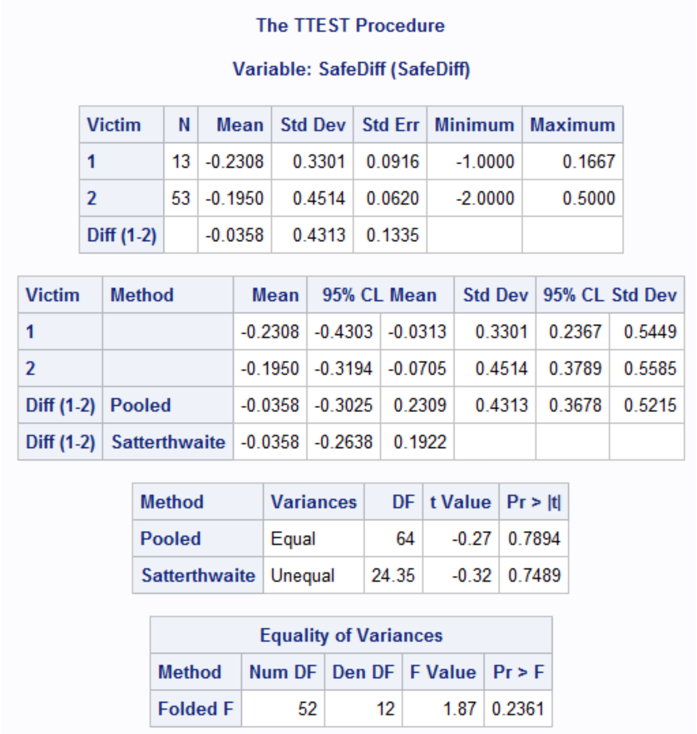
Gender	N	Mean	Std Dev	Std Err	Minimum	Maximum
1	19	-0.2281	0.3479	0.0798	-1.0000	0.1667
2	47	-0.1915	0.4597	0.0671	-2.0000	0.5000
Diff (1-2)		-0.0366	0.4312	0.1172		

Gender	Method	Mean	95% CL Mean		Std Dev	95% CL Std Dev	
1		-0.2281	-0.3957	-0.0604	0.3479	0.2629	0.5145
2		-0.1915	-0.3265	-0.0565	0.4597	0.3820	0.5774
Diff (1-2)	Pooled	-0.0366	-0.2708	0.1976	0.4312	0.3677	0.5214
Diff (1-2)	Satterthwaite	-0.0366	-0.2467	0.1735			

Method	Variances	DF	t Value	Pr > |t|
Pooled	Equal	64	-0.31	0.7560
Satterthwaite	Unequal	43.835	-0.35	0.7273

Equality of Variances				
Method	Num DF	Den DF	F Value	Pr > F
Folded F	46	18	1.75	0.1980

Differences in Victim status:



The TTEST Procedure

Variable: SafeDiff (SafeDiff)

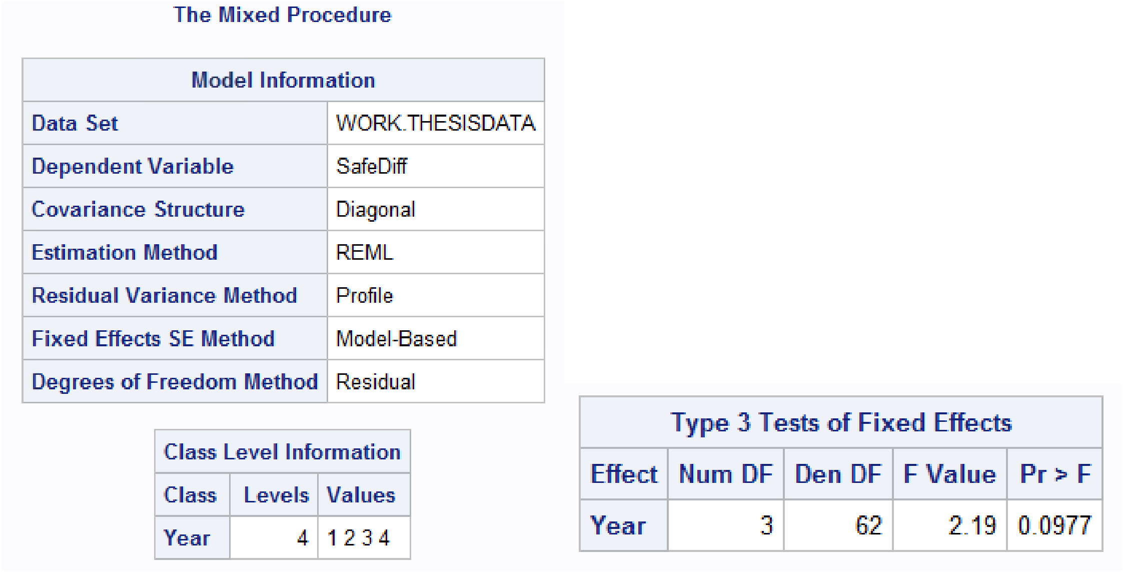
Victim	N	Mean	Std Dev	Std Err	Minimum	Maximum
1	13	-0.2308	0.3301	0.0916	-1.0000	0.1667
2	53	-0.1950	0.4514	0.0620	-2.0000	0.5000
Diff (1-2)		-0.0358	0.4313	0.1335		

Victim	Method	Mean	95% CL Mean		Std Dev	95% CL Std Dev	
1		-0.2308	-0.4303	-0.0313	0.3301	0.2367	0.5449
2		-0.1950	-0.3194	-0.0705	0.4514	0.3789	0.5585
Diff (1-2)	Pooled	-0.0358	-0.3025	0.2309	0.4313	0.3678	0.5215
Diff (1-2)	Satterthwaite	-0.0358	-0.2638	0.1922			

Method	Variances	DF	t Value	Pr > |t|
Pooled	Equal	64	-0.27	0.7894
Satterthwaite	Unequal	24.35	-0.32	0.7489

Equality of Variances				
Method	Num DF	Den DF	F Value	Pr > F
Folded F	52	12	1.87	0.2361

Differences in Year:



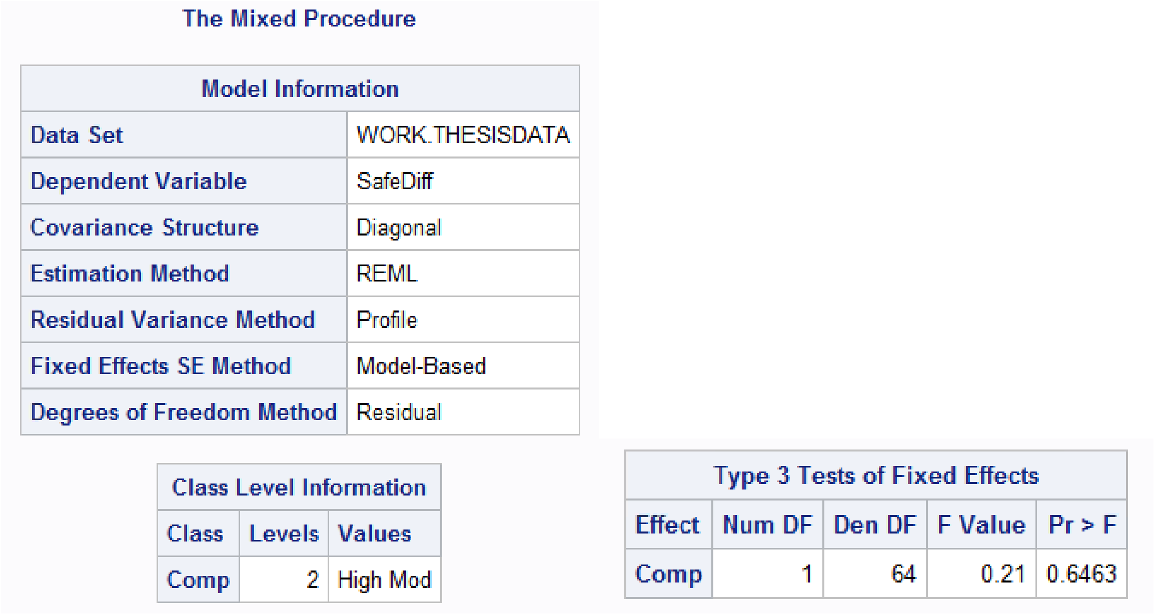
The Mixed Procedure

Model Information	
Data Set	WORK.THESISDATA
Dependent Variable	SafeDiff
Covariance Structure	Diagonal
Estimation Method	REML
Residual Variance Method	Profile
Fixed Effects SE Method	Model-Based
Degrees of Freedom Method	Residual

Class Level Information		
Class	Levels	Values
Year	4	1 2 3 4

Type 3 Tests of Fixed Effects				
Effect	Num DF	Den DF	F Value	Pr > F
Year	3	62	2.19	0.0977

Differences in Computer Knowledge:



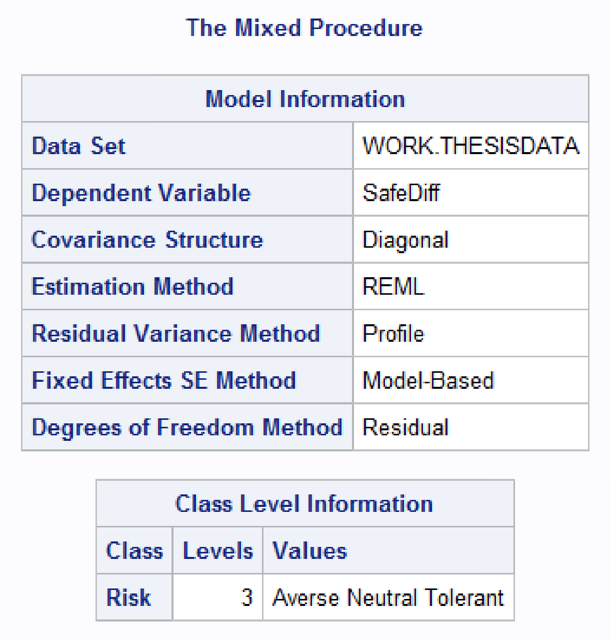
The Mixed Procedure

Model Information	
Data Set	WORK.THESISDATA
Dependent Variable	SafeDiff
Covariance Structure	Diagonal
Estimation Method	REML
Residual Variance Method	Profile
Fixed Effects SE Method	Model-Based
Degrees of Freedom Method	Residual

Class Level Information		
Class	Levels	Values
Comp	2	High Mod

Type 3 Tests of Fixed Effects				
Effect	Num DF	Den DF	F Value	Pr > F
Comp	1	64	0.21	0.6463

Differences in Risk Attitudes:

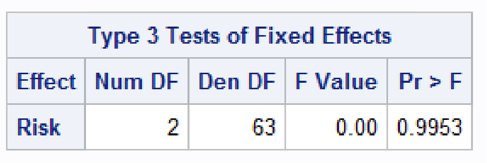


The Mixed Procedure

Model Information	
Data Set	WORK.THESISDATA
Dependent Variable	SafeDiff
Covariance Structure	Diagonal
Estimation Method	REML
Residual Variance Method	Profile
Fixed Effects SE Method	Model-Based
Degrees of Freedom Method	Residual

Class Level Information

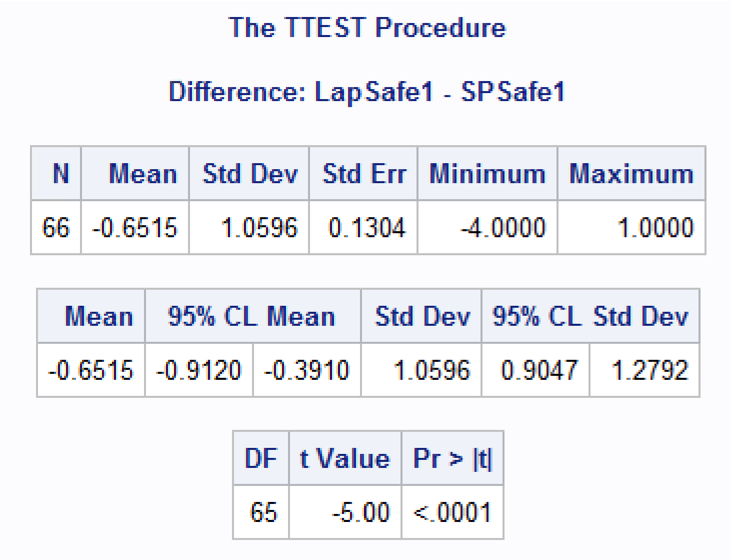
Class	Levels	Values
Risk	3	Averse Neutral Tolerant



Type 3 Tests of Fixed Effects

Effect	Num DF	Den DF	F Value	Pr > F
Risk	2	63	0.00	0.9953

Online Banking:



The TTEST Procedure

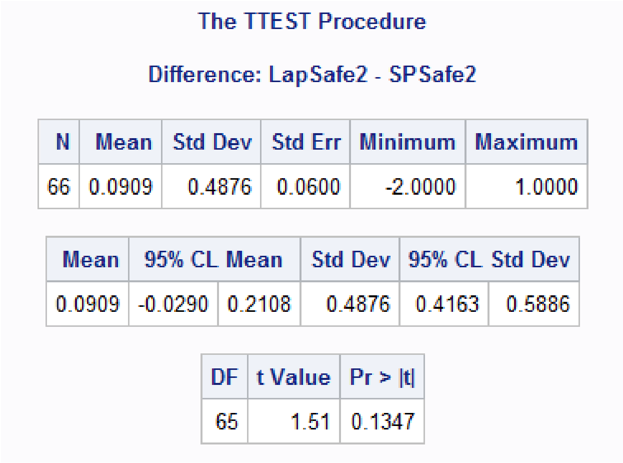
Difference: LapSafe1 - SPSafe1

N	Mean	Std Dev	Std Err	Minimum	Maximum
66	-0.6515	1.0596	0.1304	-4.0000	1.0000

Mean	95% CL Mean		Std Dev	95% CL Std Dev	
-0.6515	-0.9120	-0.3910	1.0596	0.9047	1.2792

DF	t Value	Pr > |t|
65	-5.00	<.0001

Social Networking:



The TTEST Procedure

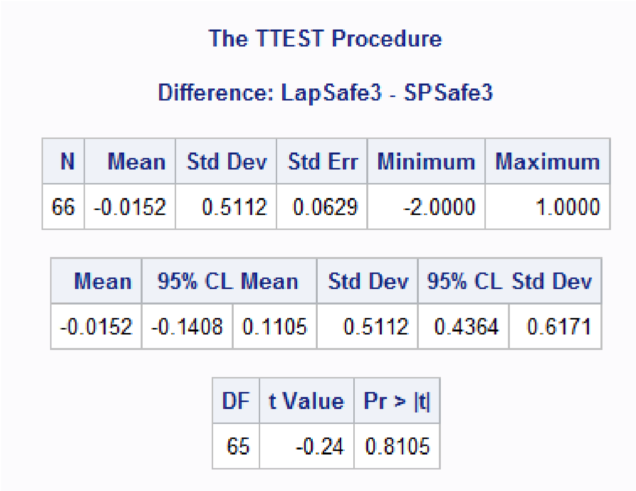
Difference: LapSafe2 - SPSafe2

N	Mean	Std Dev	Std Err	Minimum	Maximum
66	0.0909	0.4876	0.0600	-2.0000	1.0000

Mean	95% CL Mean		Std Dev	95% CL Std Dev	
0.0909	-0.0290	0.2108	0.4876	0.4163	0.5886

DF	t Value	Pr > |t|
65	1.51	0.1347

Internet Surfing:



The TTEST Procedure

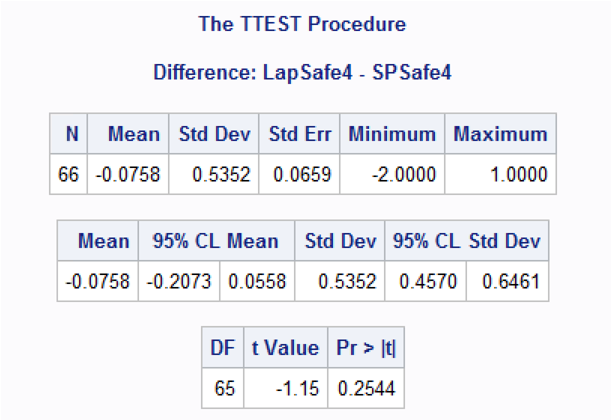
Difference: LapSafe3 - SPSafe3

N	Mean	Std Dev	Std Err	Minimum	Maximum
66	-0.0152	0.5112	0.0629	-2.0000	1.0000

Mean	95% CL Mean		Std Dev	95% CL Std Dev	
-0.0152	-0.1408	0.1105	0.5112	0.4364	0.6171

DF	t Value	Pr > |t|
65	-0.24	0.8105

Email:



The TTEST Procedure

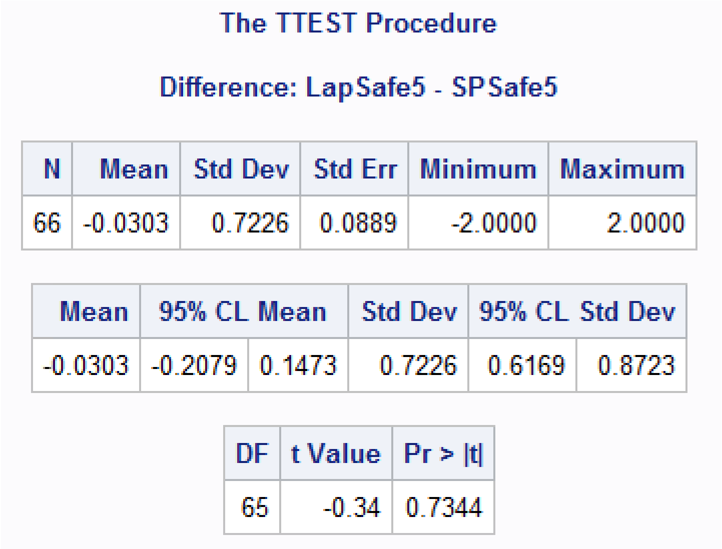
Difference: LapSafe4 - SPSafe4

N	Mean	Std Dev	Std Err	Minimum	Maximum
66	-0.0758	0.5352	0.0659	-2.0000	1.0000

Mean	95% CL Mean		Std Dev	95% CL Std Dev	
-0.0758	-0.2073	0.0558	0.5352	0.4570	0.6461

DF	t Value	Pr > |t|
65	-1.15	0.2544

Online Gaming:



The TTEST Procedure

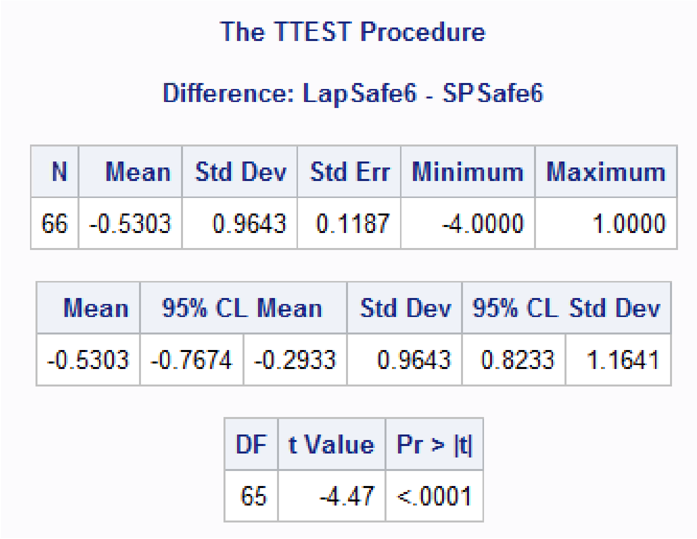
Difference: LapSafe5 - SPSafe5

N	Mean	Std Dev	Std Err	Minimum	Maximum
66	-0.0303	0.7226	0.0889	-2.0000	2.0000

Mean	95% CL Mean		Std Dev	95% CL Std Dev	
-0.0303	-0.2079	0.1473	0.7226	0.6169	0.8723

DF	t Value	Pr > |t|
65	-0.34	0.7344

E-Commerce:



The TTEST Procedure

Difference: LapSafe6 - SPSafe6

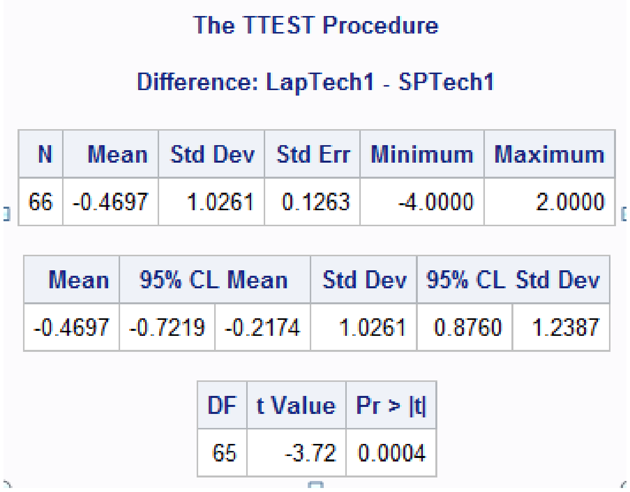
N	Mean	Std Dev	Std Err	Minimum	Maximum
66	-0.5303	0.9643	0.1187	-4.0000	1.0000

Mean	95% CL Mean		Std Dev	95% CL Std Dev	
-0.5303	-0.7674	-0.2933	0.9643	0.8233	1.1641

DF	t Value	Pr > |t|
65	-4.47	<.0001

Differences in Security Options

Password Protection



The TTEST Procedure

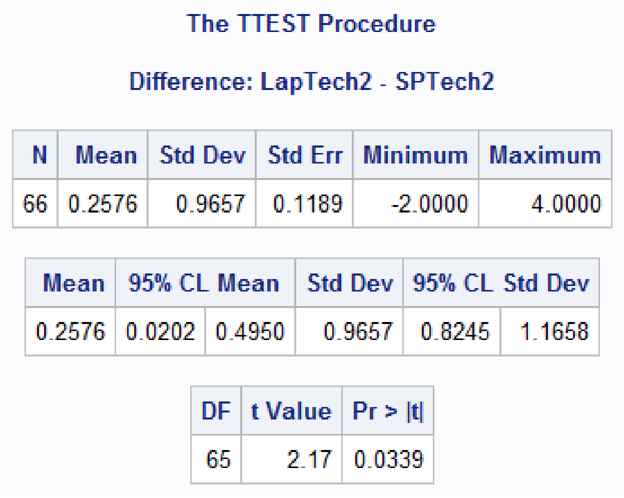
Difference: LapTech1 - SPTech1

N	Mean	Std Dev	Std Err	Minimum	Maximum
66	-0.4697	1.0261	0.1263	-4.0000	2.0000

Mean	95% CL Mean		Std Dev	95% CL Std Dev	
-0.4697	-0.7219	-0.2174	1.0261	0.8760	1.2387

DF	t Value	Pr > |t|
65	-3.72	0.0004

Remote Locate, Lock and Wipe



The TTEST Procedure

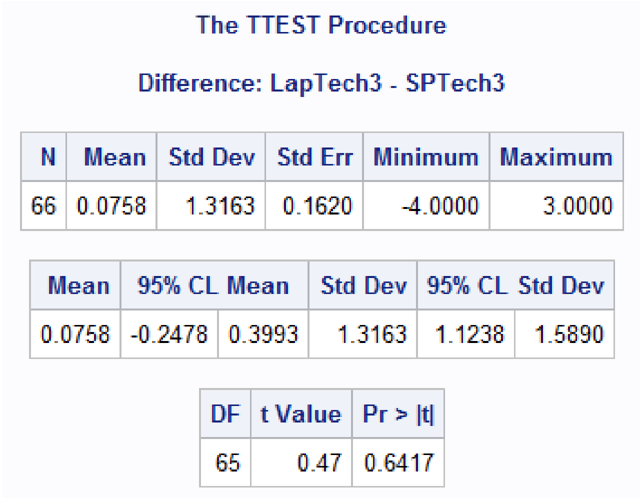
Difference: LapTech2 - SPTech2

N	Mean	Std Dev	Std Err	Minimum	Maximum
66	0.2576	0.9657	0.1189	-2.0000	4.0000

Mean	95% CL Mean		Std Dev	95% CL Std Dev	
0.2576	0.0202	0.4950	0.9657	0.8245	1.1658

DF	t Value	Pr > |t|
65	2.17	0.0339

Back-Up Data



The TTEST Procedure

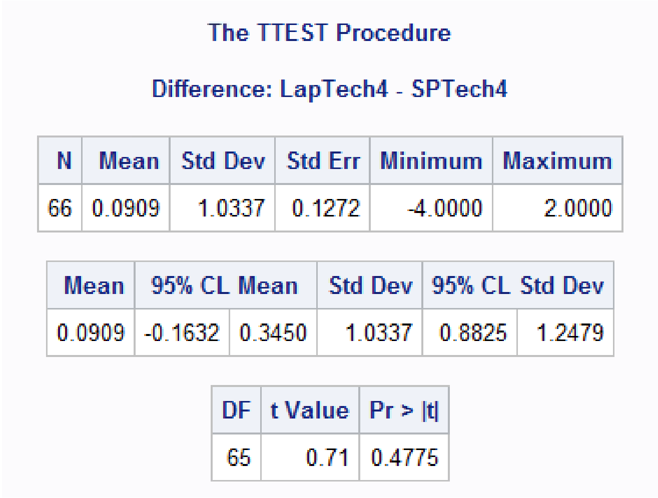
Difference: LapTech3 - SPTech3

N	Mean	Std Dev	Std Err	Minimum	Maximum
66	0.0758	1.3163	0.1620	-4.0000	3.0000

Mean	95% CL Mean		Std Dev	95% CL Std Dev	
0.0758	-0.2478	0.3993	1.3163	1.1238	1.5890

DF	t Value	Pr > |t|
65	0.47	0.6417

Apply System Updates



The TTEST Procedure

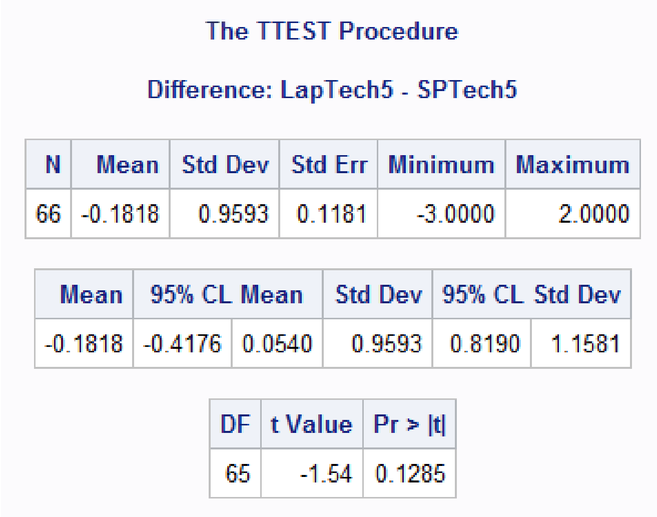
Difference: LapTech4 - SPTech4

N	Mean	Std Dev	Std Err	Minimum	Maximum
66	0.0909	1.0337	0.1272	-4.0000	2.0000

Mean	95% CL Mean		Std Dev	95% CL Std Dev	
0.0909	-0.1632	0.3450	1.0337	0.8825	1.2479

DF	t Value	Pr > |t|
65	0.71	0.4775

VPN for Wi-Fi Hotspots



The TTEST Procedure

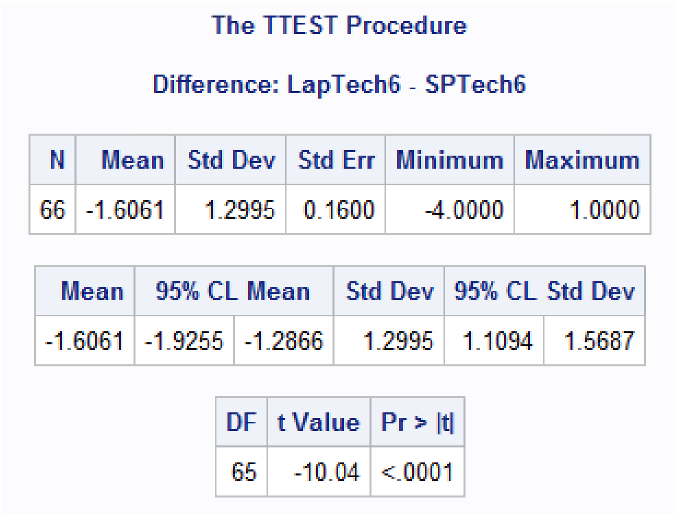
Difference: LapTech5 - SPTech5

N	Mean	Std Dev	Std Err	Minimum	Maximum
66	-0.1818	0.9593	0.1181	-3.0000	2.0000

Mean	95% CL Mean		Std Dev	95% CL Std Dev	
-0.1818	-0.4176	0.0540	0.9593	0.8190	1.1581

DF	t Value	Pr > |t|
65	-1.54	0.1285

Anti-Virus Software



The TTEST Procedure

Difference: LapTech6 - SPTech6

N	Mean	Std Dev	Std Err	Minimum	Maximum
66	-1.6061	1.2995	0.1600	-4.0000	1.0000

Mean	95% CL Mean		Std Dev	95% CL Std Dev	
-1.6061	-1.9255	-1.2866	1.2995	1.1094	1.5687

DF	t Value	Pr > |t|
65	-10.04	<.0001

BIBLIOGRAPHY

Allam, S. (2009). A model to measure the maturity of smartphone security at software consultancies. *The University of Fort Hare. Dissertation*. Retrieved from http://ufh.netd.ac.za/bitstream/10353/281/1/SA%20%28200481118%29%20Dissertation.pdf

Androulidakis, I. & Kandus, G. (2011) , Mobile phone downloading among students: The status and its effect on security," *Mobile Business (ICMB), 2011 Tenth International Conference on* , vol., no., pp.235-242, 20-21

Arthur, C. (2012). The history of smartphones: timeline. *The Guardian*, Retrieved from http://www.theguardian.com/technology/2012/jan/24/smartphones-timeline

Felt, A., Egelman S. & Wagner D. (2012). I've got 99 problems, but vibration ain't one: A survey of smartphone user's concerns. *University of California Berkeley*. Retrieved from http://www.guanotronic.com/~serge/papers/spsm12.pdf

Hulkower, B. (2013). Mobile phones- US- January 2013.*Mintel Reports*, Retrieved from http://academic.mintel.com.ezaccess.libraries.psu.edu/display/637571/

Kass, D. (2011) Smartphone users largely unaware of mobile security risks. *ITChannelPlanet.*

Retrieved from http://www.itchannelplanet.com/blog/2011/02/smartphone-users-largely-unawa.html

Mashevsky, Y. (2005). Malware evolution. *Kaspersky Lab*. Retrieved from http://www.securelist.com/en/analysis?pubid=182974451%20target=_blank

Mogg, T. (2012). Smartphone sales exceed those of PC for first time, apple smashes record. Digital Trends. Retrieved from http://www.digitaltrends.com/mobile/smartphone-sales-exceed-those-of-pcs-for-first-time-apple-smashes-record/#!BdzZD

Zhu, Z. (2012). Data service analysis, threats and countermeasures in wireless mobile environments. *The Pennsylvania State University*. *ProQuest Dissertations and Theses*, , 124. Retrieved from http://search.proquest.com/docview/1033787525?accountid=13158

ACADEMIC VITA

Kevin Laubscher
105 Arbor Creek Ct.
Chapel Hill, NC 27516
laubscherkevin@gmail.com

Education:

The Pennsylvania State University- University Park, PA
College of Information Sciences and Technology- BS in Security and Risk Analysis

Honors and Awards:

Schreyer Honors College

Association Memberships/Activities:

Phi Sigma Pi National Honors Fraternity- 2011-present
President, Executive Committee, THON chair, Initiate Advisor, Rush Chair

Professional Experience:

Liberty Mutual, Portsmouth, NH - Summer 2013
Information Technology Intern - Hosting – SecurityOps

- Aided the implementation and validation of a new intrusion prevention system and its devices
- Reviewed daily security management system reports and monitored real time events and system health

International Business Machines, Poughkeepsie, NY - Summer 2012
Data Analyst

- Statistically examined differences in post-benchmark sales between locations, brands and other categories
- Compared the actual timeline of a new system installation process to the projected timeline

Coursework:

Security Risk Analysis / Information Systems and Technology

- Cyber Forensics, Security Management, Network Security, Organization of Data, Overview of Information Security, Networking and Telecommunications, Project Management

Applied Statistics

- Applied Regression Analysis, Stochastic Modeling, Analysis of Variance, Introduction to Probability Theory