ISSN: 2454-1907
DOI: https://doi.org/10.29121/ijetmr.v5.i3.2018.201

IJETMR

International Journal of Engineering Technologies and Management Research
A Knowledge Repository

INFORMATION TECHNOLOGY USAGE: QUANTITATIVE ANALYSIS OF SMARTPHONE SECURITY AWARENESS AND PRACTICES AMONG UNDERGRADUATE STUDENTS IN THE UNITED STATES

Dr.Richmond Adebiaye [*1], Taiwo Ajani [2]

[*1] Department of Informatics and Engineering Systems, College of Science and Technology, University of South Carolina Upstate, USA

[2] Department of Computer Information Systems, Ferrum College, VA, USA

Abstract:

Mobile phone usage is growing at an unprecedented rate. The ability to remain connected, the ease of smart phone use and declining mobile costs have allowed this technology to expand at a very high rate globally. The study aimed to quantitatively determine the reasons for inactive practice of security measures of smart-phone usage among college students in the United States. The study also examined the Consideration of Future Consequences (CFC) level in relation to the level of smart-phone security measures, determined the levels of security measures on smart-phone (SP) by users, and establish the relationship between CFC level and the levels of smart-phone security measures among college students. Using a quantitative research survey and simple random sampling procedure, the methodology focused on analyzing data through testing of hypotheses. The t-test, Pearson's correlation, regression coefficients and their respective p-values. The results showed 69.8% of college students set PIN, password and screen lock on their smart phones while 74.8% were cautious with smart phone applications and 6.2% practiced on setting of security software including rooting services. On the other hand, 35.4% protected their SP data through encryption, 47.4% had data checks and security alert while 46.2% had set Bluetooth applications and 41.4% had used backup storage for sensitive data. Use of Biometrics or other security unknown security adoptions were not included in the study. The study also found that lack of knowledge about technology or applications for SP security, lack of security habits and practices, rigorous involvement of setting SP security details like backups, encryption, security software etc., assumptions that SP are security and tamper-proof as well as lack of training, guidance and after sale services on SP security are significant reasons for lack of security measures practices concerning smart-phone usage by college students.

Keywords: *Level of Practice of Security Measures of SP; SP Usage; Consideration of Future Consequences Level.*

Cite This Article: Richmond Adebiaye, and Taiwo Ajani. (2018). "INFORMATION TECHNOLOGY USAGE: QUANTITATIVE ANALYSIS OF SMARTPHONE SECURITY AWARENESS AND PRACTICES AMONG UNDERGRADUATE STUDENTS IN THE UNITED STATES." *International Journal of Engineering Technologies and Management Research*, 5(3), 270-284. DOI: https://doi.org/10.29121/ijetmr.v5.i3.2018.201.

ISSN: 2454-1907
DOI: 10.5281/zenodo.1218519

1. Introduction

Mobile communication technology (MCT) continue to expand and attain unprecedented level of usage due to several feature capabilities such as short messaging (SMS), voice messaging, gaming, social media easy access, and Bluetooth technology integration. A smart phone is a type of mobile phone that provides wireless internet access. Wireless internet access and capabilities such as text messaging, social networking, gaming, and voice messaging are powerful and alluring communication tools. Use of mobile communication gadgets like laptops, tablets and smartphones is growing at an exponential rate largely because of their ability to connect the user to internet services, their ease of application, as well as a general decline in acquisition costs to the user (Schneier, 2014). Most importantly, is the case of smartphones; from email services to short message texts, voice calls to social media usage, phonebook entries to gallery applications, the smartphone has lots of private and personal information that needs to be secured in all manners possible. As usage expands, technology companies innovate due to users' security concerns attended by high profile data breaches the society witnessed in the most recent times. However, security innovations in MCTs do not appear to be softening the impact and rate of data attacks or breaches which warrants a need for researchers to investigate the human aspect of MCT security. A typical user lacks awareness regarding security measures capable of protecting user's privacy and applications inherent to performing various tasks. The levels of smart-phone security measures among college students in USA is unclear. Thus, it is important to examine the "best security measures and practices concerning smart-phone" and determine reasons and levels for this dearth of security practices and measures,

Previous research clearly indicated that college students constitute the highest percentage of patronage among users of smartphones (Adebiaye, 2017). However, with potential prying eyes, the users of smartphones need to be extremely keen and careful to safeguard the information in their gadgets (O'Brien, 2014). Thomas (2014) describes a smartphone as a type of mobile device or phone gadget that provides wireless communication services including voice calls, short message services, and internet access among other applications. National Institute of Standards and Technology (2010) also notes that the smartphones' wireless internet access and applications such as text messaging, social networking, gaming and voice messaging are powerful and alluring communication tools that have speared most mobile device users to use such technology increasingly. However, Peppet (2014) posits that most mobile technology users lack best-practice knowledge on how to prevent and secure their gadgets from being breached or targeted by malicious mobile software threats. With rising security problems and issues with smartphones, there is a need to increase awareness about risks to personal data and mobile phone security threats. (UNDP, 2016).

2. Related Work

Modern security issues on mobile gadgets including smartphones have further-reaching effects than just losing phone contacts and short message texts when a mobile phone is lost or stolen (Fink & Segall, 2013). Potentially harmful effects on the use of smartphones are much worse when accessing the internet or social media that retain sensitive data that could be at risk if not secured. Deloitte (2016) outlines that there are several ways in which one might be putting himself or herself at risk smartphone. Recent studies by Ruggiero & Foote (2011) have shown

ISSN: 2454-1907
DOI: 10.5281/zenodo.1218519

that more than half of the smartphone users in North America do not set security details on their mobile phones. Adebiaye (2017) also concluded that these users neither set the passwords nor the personal identification numbers on their gadgets while others do not set any locking security pattern on their smartphone's keyboard. This leads to data theft, spam phone calls or registering of unwanted services that could result in financial implications. Ellada (2014) observed that one of the ways of protecting smartphones from theft and tampering is by setting password and phone pattern lock. UNDP (2016) asserts that a personal identification number (PIN) code offers a numeric alternative to security in place of a password and can also save time. However, an easy to guess password is always less secure. PINs like dates of birth (example: 1980), consecutive numbers (example: 1234) or recurring numbers (like 0000 or 5555) should be avoided. Preventing a person from being able to access a smartphone or turning it on is not enough in protecting the software of mobile phone since some information can be retrieved by plugging the smartphone into a computer or removing the SIM card. Therefore, using smartphone software that encrypts the information in files and folders is necessary (Ellada, 2014). Encryption involves standard protection, where a given code is entered before a file can be accessed, viewed or copied. Encryption may also provide security where information such as passwords, login details, account numbers and other information may be required before a file or folder is saved for online access.

Deloitte (2016) concurs with O'Brien (2014) in suggesting that one needs to be watchful of wireless networks such as Wi-Fi. Most smartphones have options for connecting to wireless networks using a wireless hotspot on the move or a router in the office/home. Wireless connections are beneficial and increase speed and efficiency of data usage but are prone to security threats. Tagert (2010) recommends that the first thing to do is to always switch off the wireless receiver when not in use, as it will save battery power and eliminates the potential risk of malicious connections to a device without your knowledge. Wireless hotspots and unknown networks are by far one of the major risks when it comes to security threats from software thieves. Deloitte (2016) explains that though Bluetooth is not seen as a potentially risky venture by most mobile users, hackers have found techniques to remotely access a smartphone within the Bluetooth range and access data from it or even browse the internet. This can be prevented setting default Bluetooth details to "non-traceable" mode. Ellada (2014) also suggests that some modern mobile devices also offer security designs that allow a range of services that automatically back up specific data to an online resource hence taking the hassle out of having to connect a phone to the computer. User's awareness can improve the use of modern security practices concerning mobile gadgets like smartphones. Therefore, this research seeks to address the security challenges regarding vulnerabilities, threats, and risks that are significant to contemporary smartphone security issues.

Purpose of the Study

The study will ultimately determine the rates of the practice of security measures of smartphone usage and examine the best security measures and practices concerning smartphone. It also aims to establish the reasons for lack of practice of security measures in smartphone usage, to examine the relations of CFC level in smartphone security against the phone security measures and finally, and to establish the relationship between CFC level and the levels of smartphone security measures amongst college students.

ISSN: 2454-1907
DOI: 10.5281/zenodo.1218519

Research Questions

1) What are the current rates of smartphone usage of smartphone security measures among college students?
2) What are the best security measures and practices regarding smartphone usage among college students?
3) What are the reasons associated with lack of practice of smartphone security measures (where they exist) among college students?
4) What are the relations of Consideration of Future Consequences (CFC) level in smartphone against their security measures among college students?
5) Is there a significant correlation between Consideration of Future Consequences (CFC) level and the rate of smartphone security measures among college students?

3. Methodology

Krueger & Casey (2000) underscore that the study methodology should include the research design, the techniques for data collection, analyzing the data and presentations of research findings. Mugenda&Mugenda (2003) and Orodho (2004) concur that the study methodology mainly focuses on the procedures and methods of analyzing data and generating the conclusions of the study.

Research Design

The study follows a quantitative research survey design which mainly focuses on: the collection of data- mostly expressed numerically through online questionnaires- and organizing and analyzing the data to generate findings of the study. The research will also help in testing the hypotheses on- the reasons behind the lack of practice of security measures of smartphone usage as well as the correlation between Consideration of Future Consequences (CFC) level and the rate of smartphone security measures among college students.

Study Variables

The study variables are grouped into three broad categories: response variable, explanatory variables, and confounding variables. The response (dependent) variable of the study is the level of smartphone security measures and practices. The explanatory (independent) variables include – Consideration of Future Consequences (CFC) level, smartphone IT characteristics, Smartphone user satisfaction, perceived smartphone ease of use, modern best practices on smartphone security and usage and the reasons behind the lack of practice of security measures on smartphone usage. The confounding variables include personal demographic attributes such as – age, gender, smartphone IT experience, year of study and socio-economic status of cyber-security practitioners.

Data Collection

The study targeted all college students using smartphones and smartphone in the USA. Due to lack of time and limited resources, a sample size of 215 college students was evaluated for this research. An online survey-style questionnaire was used as a research instrument for this particular study as it sought to give insights concerning the smartphone security practices and measures. The online survey-styled questionnaires had some questions with choices scaled using the 5-point Likert scale. The Likert scale had choices: Strongly Disagree (SD=1), Disagree

ISSN: 2454-1907
DOI: 10.5281/zenodo.1218519

(D=2), Neutral (N=3), Agree (A=4) and Strongly Agree (SA=5). The online survey-styled questionnaires were found to be valid, reliable and achievable in providing information for generalizations.

Data Analysis Procedure

The socio-demographic data of the respondents was organized using descriptive statistics, frequency tables, and graphical methods. The data concerning the research questions were analyzed using: descriptive statistics, students t-tests, Pearson's correlations and multiple regression analysis. The student t-test values (t), Pearson's correlation coefficient (r), regression coefficients (B) and their respective p-values were used to evaluate the research data. The results were then summarized and interpreted to generate the findings of the study. The data analysis was mainly completed using social package for social scientists (SPSS version 22).

4. Results

This section presents data analysis on socio-demographic factors of respondents as well as the analysis of research hypotheses

4.1. Analysis of Socio-Demographic Factors

Table 1: Frequency Distribution and descriptive statistics of demographic factors

Variable	Attribute	Frequency	Percent	Mean	Standard Deviation
Age	15	15	7.0	16.67	0.81
	16	73	34.0		
	17	95	44.2		
	18	32	14.9		
	Total	215	100.0		
Gender	Male	114	53.0	1.47	0.50
	Female	101	47.0		
	Total	215	100.0		
Year of Study	First	79	36.7	1.83	0.74
	Second	93	43.3		
	Third	43	20.0		
	Total	215	100.0		
Smartphone IT experience	Basic	21	9.8	2.92	1.00
	Intermediate	54	25.1		
	High	61	28.4		
	Masterly	79	36.7		
	Total	215	100.0		
Socio-economic status	Low	54	25.1	2.08	0.76
	Middle	89	41.4		
	High	72	33.5		
	Total	215	100.0		

ISSN: 2454-1907
DOI: 10.5281/zenodo.1218519

Table 1 shows that 53.0% of the respondents who participated in the study of lack of security measures in smartphone usage were males, while 47.0% were females. These results show that there was gender disparity among the smartphone usage as displayed in the pie chart below.

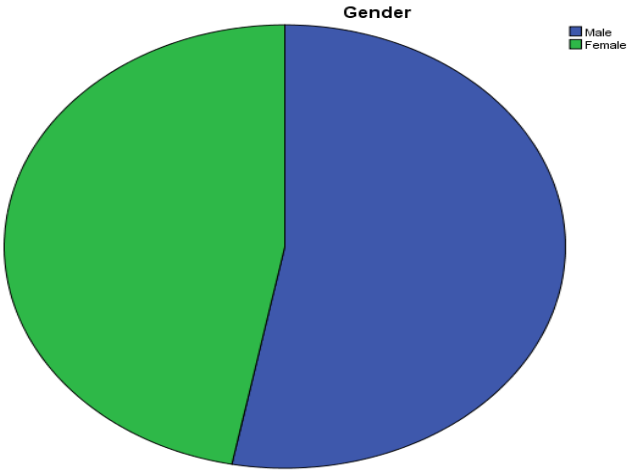

Figure 1: Pie chart showing gender distribution

Concerning the age of respondents, most of the college students were 17 years old with a relative frequency of 44.2%, followed by those who are aged 16 years with a relative frequency of 34.0%. Those aged 18 years and 15 years were minor groups with relative frequencies of14.9% and 7.0% respectively. The age of respondents displayed a normal curve as shown in the histogram below.

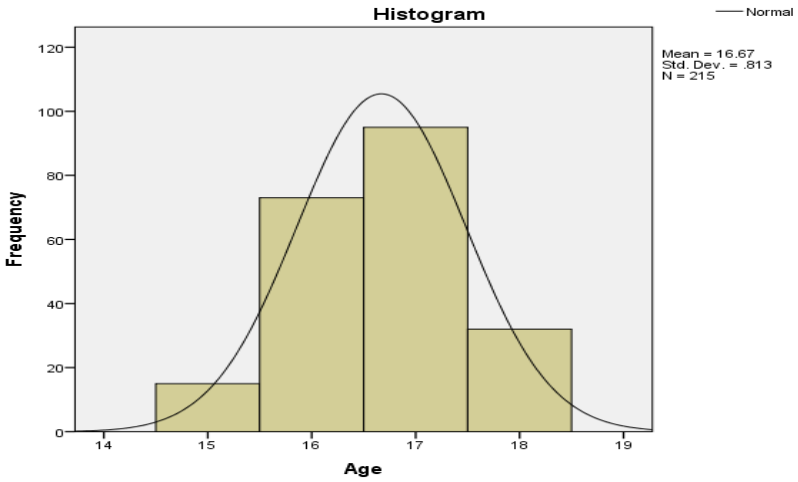

Figure 2: Histogram showing age distribution

The study also inquired about the respondents' year of study in their college education. The results in table 1 show that 43.3% of the respondents were second-year students, 36.7% were first-year students and 20.0% were third-year students at colleges. These results showed that majority of the respondents were second-year students as portrayed in the bar graph below.

ISSN: 2454-1907
DOI: 10.5281/zenodo.1218519

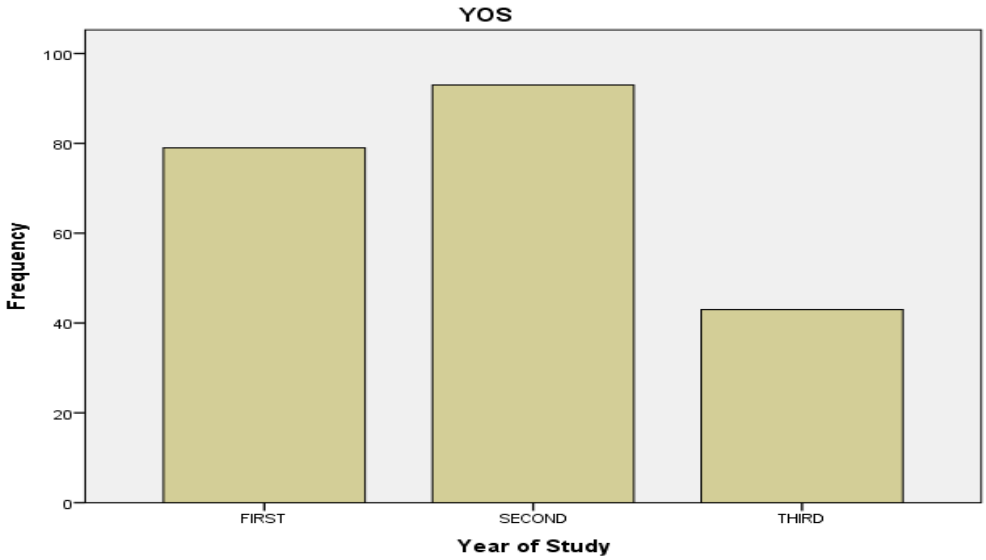

Figure 3: Bar graph showing year of study distribution

Table 1 results also indicated that most participants in the study had masterly smartphone IT experience (36.7%) followed by those having high smartphone IT experience (28.4%). The other smartphone IT experience groups were intermediate and basic with relative frequencies of 25.1% and 9.8% respectively. The bar graph below shows that there is an increase in the frequency of college students with increase in smartphone IT experience.

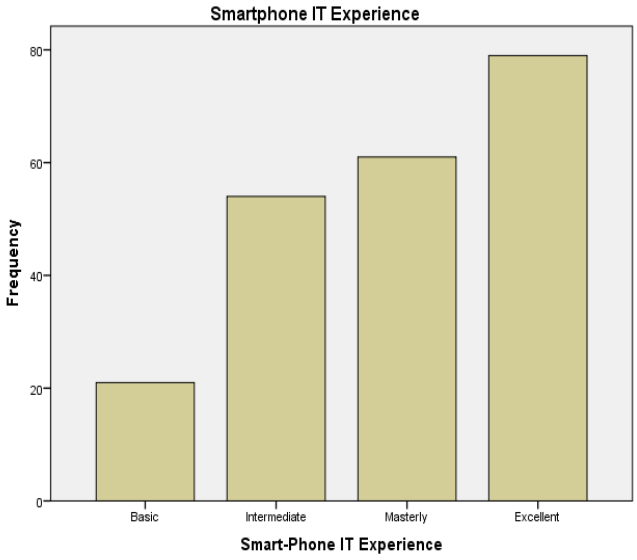

Figure 4: Bar graph showing Smartphone IT experience distribution

Concerning the participants' socio-economic status, results indicated that; 41.4% of respondents had middle-level socio-economic status, followed by 33.5% who are of high socio-economic status and lastly, 25.1% are of low socio-economic status. These results showed most

ISSN: 2454-1907
DOI: 10.5281/zenodo.1218519

respondents are of middle socioeconomic status. The pie chart below shows the results of the socio-economic status of the respondents.

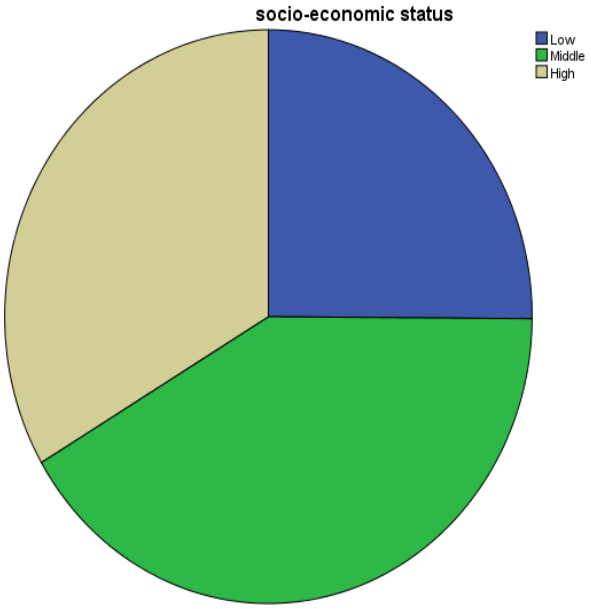

Figure 5: Pie chart showing Socio-economic status distribution

5. Discussion: Analysis Concerning The Research Objectives

This section used quantitative analysis to determine the reasons behind the lack of practice of security measures of smartphone (SP) usage as well as examine the Consideration of Future Consequences (CFC) level in correlation to the level of smartphone security measures among college students. The analysis will help in answering the following research objectives and hypotheses.

5.1. The Current Rate of Practice of Security Measures of Smartphone (SP) Usage

The current rates of practice of security measures of smartphone usage among college studentswereanalyzed using sample descriptive statistics (means and standard deviations). The following research question was helpful in carrying out the analysis.

RQ1: What are the current rates of the practice of security measures of smartphone usage among college students?

Table 2: Sample descriptive Statistics

Variable	N	Mean	Mean (%)	Std. Deviation	Std. Error Mean

ISSN: 2454-1907
DOI: 10.5281/zenodo.1218519

Overall Smartphone Security Level	**215**	**3.39**	**67.8**	**.495**	**.028**
Setting PIN, Password and Screen lock	215	3.49	69.8	.501	.034
Protection through encryption	215	1.77	35.4	.404	.024
Wireless checks and security alert	215	2.37	47.4	.484	.033
Bluetooth Security applications	215	2.31	46.2	.253	.029
Cautious with SP applications	215	3.74	74.8	.534	.041
Setting backup storage for sensitive data	215	2.07	41.4	.484	.033
Setting security software including rooting services	215	3.31	66.2	.423	.029

The results show that the overall smartphone security level (μ=3.39 and σ=0.495) has a mean of 3.39 out of possible 5 indicating that about 67.8% of the students in colleges have security measures in place on their smartphones. The results also indicate that setting PIN, password, and screen lock (μ=3.49 and σ=0.501), being cautious with smartphone applications (μ=3.74 and σ=0.534) and the setting of security software including rooting services (μ=3.31 and σ=0.423) are above average in terms of security practices and measures of smartphone usage. These security practices and measures of the smartphone are rated to above 50% in usage among college students.

It is however noted that security practices and measures of smartphone usage like: protection through encryption (μ=1.77 and σ=0.404), wireless internet checks and security alert (μ=2.37 and σ=0.484), Bluetooth security applications (μ=2.31 and σ=0.253) and setting backup storage for sensitive data (μ=2.07 and σ=0.484) were below average in terms of security practices and measures of smartphone usage. These security practices and measures of the smartphoneare rated below 50% in usage among college students.

5.2. Modern Security Features and Practices Concerning Smartphone (SP) Usage

Modern security features andpractices concerning smartphone usage among college students were analyzed using both sample descriptive statistics and students t-test. The following research hypothesis was used to guide the test.

Table 3: One-Sample t-test Statistics

Variable	**N**	**Mean**	**Std. Deviation**	**Test Value = 2.5**		
				t	**df**	**Sig. (2-tailed)**
Setting PIN, Password and Screen locks	215	3.49	.501	29.056	214	.000
Protection through encryption	215	1.77	.304	-4.391	214	.092
Wireless checks and security alert	215	2.37	.484	-16.393	214	.000
Bluetooth Security applications	215	2.31	.253	-14.712	214	.000
Cautious with Smartphone applications	215	3.74	.534	32.340	214	.000
Setting backup storage for sensitive data	215	2.07	.484	-6.393	214	.068

ISSN: 2454-1907
DOI: 10.5281/zenodo.1218519

Setting security software including rooting services	215	3.31	.423	21.198	214	.000
Overall Smartphone Security Level	**215**	**3.39**	**.495**	**31.786**	**214**	**.000**

Table 3 results indicate that the overall smartphone security level (t=31.786 & p=0.000) is significant in terms of modern best security measures and practices concerning smartphone usage. Other significant modern best security measures and practices concerning smartphone usage among college students are: Setting PIN, password and screen locks (t=29.056 & p=0.000), wireless checks and security alert (t=-16.393 & p=0.000), Bluetooth security applications (t=-14.712 & p=0.000), cautious with smartphone applications (t=32.340 & p=0.000) and setting security software including rooting services (t=21.198 & p=0.000).The results also show that; protection through encryption (t=21.198 & p=0.000) and setting backup storage for sensitive data (t=21.198 & p=0.000) are not significant modern best security measures and practices concerning smartphone usage among college students.

5.3. The Reasons For Lack of Practice of Security Measures in Smartphone (SP) Usage

The reasons for lack of practice of security measures of smartphone usage among college students were analyzed using both sample descriptive statistics and students t-test.

Table 4: One-Sample t-test Statistics

Variable	**N**	**Mean**	**Std. Deviation**	**Test Value = 2.5**		
				t	**df**	**Sig. (2-tailed)**
Lack of knowledge and technology on SP security	215	2.38	.799	-20.624	214	.000
Lack of security habits and practices	215	2.54	.924	-15.246	214	.008
Not aware of SP security threats	215	3.39	1.248	-1.284	214	.200
General negligence and laxity on SP security usage	215	4.37	2.484	6.393	214	.150
Due to involving nature of setting SP security details...	215	2.94	.924	17.298	214	.001
Assuming that SP are security and tamper-proof	215	3.49	.501	29.056	214	.000
Lack of training, guidance and after sale services on SP security	215	3.13	.991	17.982	214	.000

Table 4 results indicate that lack of knowledge and technology on SP security (t=-20.624 & p=0.000), lack of security habits and practices (t=-15.246 & p=0.008), due to the involving nature of setting SP security details like backups, encryption, security software etc. (t=17.298 & p=0.001), assuming that SP are security and tamper-proof (t=29.056 & p=0.000) and lack of training, guidance and after sale services on SP security (t=17.982 & p=0.000) are significant in terms of reasons for lack of practice of security measures of smartphone usage. The results also show that lack of awareness of SP security threats (t=-1.248 & p=0.200) and general negligence

ISSN: 2454-1907
DOI: 10.5281/zenodo.1218519

and laxity on SP security usage (t=6.393 & p=0.150) are not significant reasons for lack of practice of security measures concerning smartphone usage among college students.

5.4. The Consideration of Future Consequences (CFC) Level in Smartphone Security Measures

The relations of Consideration of Future Consequences (CFC) level in smartphone against their security measures among college students was analyzed using Pearson's correlation coefficients and their respective p-values. The following research question was used in carrying out the test.

RQ4: What are the relations of Consideration of Future Consequences (CFC) level in smartphone against their security measures among college students?

Table 5: Correlations

		CFC Level	**Smartphone Security Level**	**Perceived Ease of Use (PEOU)**	**Smartphone's Characteristics &Applications**	**Smartphone User Satisfaction**
CFC Level	r	1	.719**	.665**	.488**	.574**
	Sig.		.000	.000	.000	.000
	N		215	215	215	215
Smartphone Security Level	r		1	.979**	.650**	. 802**
	Sig.			.000	.000	.000
	N			215	215	215
Perceived Ease of Use (PEOU)	r			1	.492**	.879**
	Sig.				.000	.000
	N				215	215
Smartphone's Characteristics & Applications	r				1	.647**
	Sig.					.000
	N					215
Smartphone User Satisfaction	r					1
	Sig.					
	N					

Table 5 results show that the CFC level is significantly and strongly correlated to Smartphone Security Level (r=0.719, p=0.000) and Perceived Ease of Use, PEOU (r=0.665, p=0.000). On the other hand, the CFC level is significantly but moderately correlated to: Smartphone's Characteristics & Applications (r=0.488, p=0.000) and Smartphone Use Satisfaction (r=0.574, p=0.000). Therefore, the Consideration of Future Consequences (CFC) level in a smartphone is significantly related to smartphone security measures and features in usage among college students. Table 5 also shows that the Smartphone Security Level is significantly and strongly correlated to: CFC level (r=0.719, p=0.000), the Perceived Ease of Use, PEOU (r=0.979, p=0.000) the Smartphone's Characteristics & Applications (r=0.650, p=0.000) and Smartphone Use Satisfaction (r=0.802, p=0.000). Therefore, the Smartphone Security Level is significantly related to smartphone security features and CFC level in smartphone usage among college students.

ISSN: 2454-1907
DOI: 10.5281/zenodo.1218519

5.5. The Relationship Between Smartphone Security Measures Level and CFC Level

The relationship between the rate of smartphone security measures and practices against Consideration of Future Consequences (CFC) level among college students was analyzed using multiple regression analysis based on t-values (t), beta values (B) and their respective p-values (p).

Table 6: Multiple Regression Analysis

Model		Unstandardized Coefficients		t	Sig.
		B	Std. Error		
1	(Constant)	.465	.053	16.436	.000
	Consideration of Future Consequences (CFC) Level	.285	.009	13.360	.007
	Perceived Ease of Use (PEOU)	.691	.019	42.743	.000
	Smartphone's Characteristics & Applications	-.518	.013	-39.493	.000
	Smartphone User Satisfaction	.817	.015	60.133	.000
a. Dependent Variable: Smartphone Security Level					

Table 6 results indicate that all the four explanatory variables (Consideration of Future Consequences (CFC) Level, Perceived Ease of Use (PEOU), Smartphone's Characteristics & Applications and Smartphone User Satisfaction) are significant in explaining the Smartphone Security Level for college students. The significance of the four explanatory variables are: Consideration of Future Consequences (CFC) Level (t=13.360, p=0.007), Perceived Ease of Use (PEOU) (t=42.743, p=0.000), Smartphone's Characteristics & Applications (t=-39.493, p=0.000) and Smartphone User Satisfaction (t=60.133, p=0.000).The regression coefficient (beta values) in table 6 results show how an increase in consideration of future consequences (CFC) Level by one will lead to increase in Smartphone Security Level by 0.285 (B=0.285) provided other factors are held constant. On the other hand, when perceived ease of use of a smartphone increased by one the Smartphone Security Level will increase by 0.691 (B=0.691). Results also show that an increase in smartphone's characteristics and applications will simultaneously increase the smartphone security level by 0.518 (B=-0.518). Finally, a one level increase in smartphone user satisfaction will also increase the smartphone security level by 0.817 (B=0.817). Finally, since all the p-values are less than 0.05, we reject the null hypothesis and conclude that there is significant relationship between the smartphone security measures and practices level on one hand and; consideration of future consequences (CFC) Level, Perceived Ease of Use (PEOU), Smartphone's Characteristics and Applications and Smartphone User Satisfaction on the other side in usage among college students.

6. Findings and Conclusions of the Study

Findings from table 2 results show that 69.8% of college students set PIN, password and screen lock while 74.8% of the sampled population were found to be cautious with smartphone applications. About sixty-six percent (66.2%) practiced setting of security software including rooting services. Therefore, the study concludes that setting PIN, password and screen lock (μ=3.49), being cautious with smartphone applications (μ=3.74) and setting off security software including rooting services (μ=3.31) were above average in terms of security practices and measures of smartphone usage among college students. Conversely, the study also found that

ISSN: 2454-1907
DOI: 10.5281/zenodo.1218519

security practices and measures like: protection through encryption (35.4%), wireless internet checks and security alert (47.4%), Bluetooth security applications (46.2%) and setting backup storage for sensitive data (41.4%) were rated as below average in terms of security practices and measures of smartphone usage among college students. The study also found that most modern security measures and practices concerning smartphone usage among college students tested were significant best security measures and practices concerning smartphone usage. Since their p-values were less than 0.05.The study concludes that: setting PIN, password and screen locks, wireless checks and security alert, Bluetooth security applications, cautiousness with smartphone applications and setting security software including rooting services are significant modern best security measures and practices concerning smartphone usage among college students.

The study found that five out of the seven reasons college students lack security measures concerning smartphone usage are significant since they had p-values that were less than 0.05. The study indicated that: lack of knowledge and technology on smartphone security, lack of security habits and practices, the involving nature of setting smartphone security details like backups, encryption, security software etc., assumptions that smartphone is secure and tamper-proof as well as lack of training, guidance and after sale services on smartphone security were strong factors for lack of practice of security measures of smartphone usage among college students. The study also found the existence of a strong relationship between smartphone security measures and practices level on the one hand and; Consideration of Future Consequences (CFC) Level, Perceived Ease of Use of smartphone, smartphone's characteristics & applications and smartphone user satisfaction on the other, in usage among college students. The study, therefore, concludes that Consideration of Future Consequences (CFC) level, perceived ease of use of a smartphone, smartphone's characteristics & applications and smartphone user satisfaction are significant predictors of smartphone security measures' levels. The study also found that the regression coefficients can be used to quantify the effects of the significant predictors of smartphone security measures' levels. The results show that an increase in Consideration of Future Consequences (CFC) level by one will lead to increase in smartphone security level by 0.285 (B=0.285) provided other factors are held constant. When perceived ease of use of smartphone increases by one, the smartphone security level will increase by 0.691 (B=0.691) while when Smartphone's characteristics & applications increase by a factor of one the smartphone security level will decrease by 0.518 (B=-0.518). Finally, when smartphone user satisfaction increases by a factor of one the smartphone security level increases by 0.817 (B=0.817).The study also examined the relationship between the smartphone security level (response variable) against; Consideration of Future Consequences (CFC) Level, perceived ease of use of a smartphone, smartphone's characteristics & applications and smartphone user satisfaction (explanatory variables) using a regression equation shown below.

$$\textbf{SPS Level} = 0.465 + 0.285 * \textbf{CFC} + 0.691 * \textbf{PEOU} - 0.518 * \textbf{SPCA} + 0.817 * \textbf{SPUS}$$

Where;
SPS Level is Smartphone security level
CFC is Consideration of Future Consequences
PEOU is Perceived Ease of Use of Smartphone
SPCA is Smartphone's Characteristics & Applications
SPUS is Smartphone User Satisfaction

ISSN: 2454-1907
DOI: 10.5281/zenodo.1218519

Finallythe study found a significant relationship between the smartphone security measures and practices level and, Consideration of Future Consequences (CFC) Level, Perceived Ease of Use (PEOU), Smartphone's Characteristics & Applications and Smartphone User Satisfaction.

References

[1] Adebiaye, R. Mitigating Vulnerability Risks in Cyber security Using Predictive Measures, International Journal of Advanced Scientific Research & Development. 4(10/I), 2017, 12-26.
[2] Adebiaye, R. Interpreting User's perceptions of Mobile Security Methods and Their Effectiveness, International Journal of Engineering and Advanced Technology. 6(4), 2017, 01-18.
[3] Adebiaye, R., Alryalat, H., and Owusu, T. Perspectives for Cyber-Deterrence: A Quantitative Analysis of Cyber Threats and Attacks on Consumers, International Journal of Innovative Research in Science, Engineering and Technology. 5(7), 2016, 01-18.
[4] Barcena, M. B. et al. Security Response: How safe is your quantified self? Journal of International Communication. 10(2), 2014, 180-211.
[5] Center for Strategic and International Studies. Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II. CSIS. 2014.
[6] Deloitte. Cybercrime: The current landscape and the hidden costs. Dubai: Deloitte Corporate Finance Limited. 2016.
[7] Ellada, G. Cyber security in developing countries, a digital divide issue, Journal of International Communication. 20(2), 2014, 200-217.
[8] Fink, E. &Segall, L. Your TV might be watching you. CNN MONEY.2013. Available at: http://money.cnn.com/2013/08/01/technology/security/tv-hack/index.html
[9] Graham D. Computer Security Incident Handling Guide (Trans: Computer Security Division ITL). NIST Special Publication. National Institute of Standards and Technology, Gaithersburg, MD. 2013.
[10] Kothari, C.R. Research Methodology and Techniques; 2ndedition. New Delhi. New York. New Age International Publishers. 2004.
[11] Krueger, A. and Casey, M.A. Focus Groups: A Practical Guide for Applied Research 3rd. ed. Thousand Oaks, C.A, Sage.2000.
[12] Mugenda,O.M.and Mugenda,A.G. Research methods. Qualitative and quantitative approaches. Nairobi: Acts Press. 2003.
[13] National Institute of Standards and Technology. Guidelines on Cell Phone and PDA Security (SP 800-124). 2014. Available at:http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf
[14] O'Brien, D. The Internet of Things: New Threats Emerge in a Connected World, SYMANTEC. 2014. Available at: www.symantec.com/connect/blogs/internet-thing-new-threats-emerge-connected-world
[15] Orodho,J.A. Elements of Education and Social Sciences Research Methods.Nairobi.Bureau Education Research. Masola Publishers. 2004.
[16] Peppet, S. R. Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent. 93(85), 2014, 115-126.
[17] Ruggiero, P. and Foote, J. Cyber Threats to Mobile Phones. US Computer Emergency Readiness Team (US-CERT). Carnegie Mellon University, Washington USA. 2011.
[18] Schneier, B. The Internet of Things Is Wildly Insecure And Often Unpatchable. 2014. Available at: http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem
[19] Schneier, B. The Internet of Things Is Wildly Insecure and Often Unpatchable, SYMANTEC. (Version 1.1). 2014. Available at:

ISSN: 2454-1907
DOI: 10.5281/zenodo.1218519

www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/how-safe-is-your-quantified-self.pdf

[20] Tagert, A.C. Cyber security Challenges in Developing Nations. Dissertations. Paper 22. 2010.

[21] Thomas, P. Despite the News, Your Cellphone is Not Yet Sending Spam, SYMANTEC. 2014. Available at: http://www.symantec.com/connect/blogs/despite-news-your-cellphone-not-yet-sending-spam

[22] UNDP. UNDP Smartphone and Cyber security practices for developing nations. New York: UNDP. 2016.

[23] Wilcox, R. Introduction to Robust Estimation and Hypothesis Testing (Ed.2). 2005, 3-17.

*Corresponding author.
E-mail address: Radebiay@ uscupstate.edu