Critical Analysis of Mobile Phone Communication Safety and Security Measures: Familiarity versus Actual Practice on Mobile Devices

Ewuuk Lomo-David
lomoe@ncat.edu
School of Business and Economics
North Carolina A&T State University
Greensboro, NC 27411

Li-Jen Shannon
Lys001@shsu.edu
Department of Computer Science
Sam Houston State University
Huntsville, TX 77341

Abstract

The use of mobile communicating devices such as mobile phones has become one of the most popular contemporary methods of exchange of information in the world. Since Nigeria is currently Africa's largest mobile phone market subscriber, the focus of this study was to evaluate how university students (prospective employees) in Nigeria (Africa's most populous country) use and manage mobile phone devices safety and security measures. An interesting finding in this study is that respondent's age, academic major, prior knowledge/experience with computers and the number of hours they had waited for their mobile phone device to be repaired after a malfunction directly affect their level of familiarity and usage of mobile phone safety and security measures. A very low percentage of students take steps to safeguard and use passwords on their mobile phones. Furthermore, this study could provide guidelines and strategies to help avoid and reduce falling prey to insecurities associated with cyber-crimes and target areas requiring security emphasis for students.

Keywords: familiarity versus practice of mobile phone communication safety, Nigerian information security, biometric security, students' password use.

1. INTRODUCTION

Definitions: We define mobile communication devices to include smart mobile phones, laptops, notebooks, Personal Digital Assistants (PDAs) that are collectively used for internet interaction, person to person or business to business communication etc. The primary focus of this study is mobile phones; defined as an integrative mobile terminal capable of processing digital data, voice, video etc. and interfacing through a personal area network (PAN) or wide area network (WAN) with other receiving terminals.

Contemporary ubiquitous mobile phone communication technologies provide a multiplicity of ways to connect to the world in the twenty-first century. The use of mobile communication devices such as cellular phones is one of the de facto methods to exchange information in corporate and educational settings, connect with friends and families, business

associates and also retrieve the latest news, sports, weather, etc. In early 2008, Nigeria (Africa's most populous country) overtook South Africa and became Africa's largest mobile phone market with over 44 million subscribers (Africa Research Report, 2008). Cable News Network (CNN) News also reported that Africa had the highest growth in mobile phone device use globally. This growth was twice the global average over the past three years (Water, 2008). Recent reports placed Nigerian mobile phone subscriber base at 68 million (Ohuocha, 2009; Ghana Business News, 2009). That is an increase of 24 million subscribers between early 2008 and first quarter of 2009. Currently the following established four private mobile phone companies operate in Nigeria: MTN, Globacom, Etisalat, and Zain (formerly Celtel). This number may increase as Nigeria plans the sale of its own Nigerian Telecommunications Ltd (NITEL) (Okolo, 2009) and allows other mobile companies to prospect the possibility of entering the Nigerian mobile phone market.

With a fast growing network usage, two of the biggest problems facing internet development in Africa are lack of interconnectivity (Water, 2008) and maintaining safety and security of data. While many African countries looked for resolutions in hardware infrastructure, we believe that the basic concepts of information security and safety issues at the entry levels should be emphasized as well. Since the September 11, 2001 (911) tragedies happened, USA had been implementing many homeland security projects (physical and digital) to protect our country and citizens. The success of these security implementations has far-reaching effects in this country as well as in Nigeria and other parts of the world. One of many worthwhile projects was cyber-crime prevention. Many studies indicate that cyber-crimes threaten this country's physical, digital and socio-economic security. Estimating the cost of cyber-crime is futile (Grabosky, 2005) because a large number of these crimes are not reported. Public knowledge of some of these cases are even legally suppressed as reported in a multimillion dollar settlement reached by two companies in Idaho in 2008 in which the terms of the settlement precluded public identifications of the litigants. One of the companies hacked into the other's database to steal valuable information (Shifrin, 2008). Estimates suggest that the economic impact of virus attacks on information systems around the world amounted to US$12.1 billion in 1999 and US$ 17.1 billion in 2000 (Grabosky, 2005). The importance of ensuring that information is protected in this society cannot be over emphasized "because information processes straddle all our day-to-day processes and transactions; including business, education, health care, and all other aspects of life" (Kizza & Kizza, 2008). In fact, the focus on information protection should rightfully shift to include Africa because of the enormous digital growth being experienced in a continent of almost a billion people (Wikipedia, 2008). The security and safety risk associated with Nigeria (as well as Africa) mobile phone market leaves a gaping hole for criminal activity because the purchase of a mobile phone does not require a registration as in U.S. and Europe. Because of this pay-as-you-go mobile phone use mentality and the lack of registration, a stolen or missing mobile phone cannot be traced to anybody. Criminal activity conducted with a mobile phone cannot be traced to a specific and known subscriber. Nigeria Communications Commission (NCC) should require the registration of all mobile phones sold, bought and used in Nigeria, in order to create traceability to specific phones and registrants in case of criminal activity. In fact, if mobile phone companies in Africa resist the registration and identification of each mobile phone sold, these companies should be held responsible when criminal activity in which the company's server and phone was involved.

To forestall continuous proliferation of mobile phone information systems insecurity and negative economic impact on African countries in the future, this study was designed to investigate and evaluate the threshold of familiarity and the levels at which university students (prospective employees) actually practice safe mobile communication and computing.

2. RELATED LITERATURE

Mobile Communication With Information Security Measures

Throughout the rapid technological developments in the last two decades, wireless technology has been seen as one of the fastest developing technologies of the communication industry. Kizza and Kizza (2008) stated that wireless technology is based on a concept of a cell which became the underlying technology for mobile telephones, personal communication systems, wireless Internet, and wireless Web applications. Each cell has a communication tower called the base station (BS) that communication devices use to transmit data via satellite. Each BS operates two types of channels:

1. The control channel, which is used in the exchange when setting up and maintaining calls
2. The traffic channel, which carries voice/data (Kizza & Kizza, 2008, p. 262).

Most internet service providers are active in (wireless) WiFi and experiment with wimax (long-distance wireless) technologies, offering Internet through satellite and exploring the new 3G mobile phone generation. In the years 2004 and 2005, mobile Internet services were already responsible for a substantial part of the growth of mobile services in general (Kung, Picard, & Towse, 2008).

Many companies have been providing various services to satisfy their customers' needs. These services include mobile advertisement, marketing, music, gaming, video, network, and many others. To secure the mobile servers and protect the customers' privacy, many options are available through each mobile internet service. The most common protection types are access control and authentication.

Access Control

Access control is the frontline of system security. "Access control mechanisms help in limiting access to system resources by any unauthorized attempted access, including malicious code, copying of data, illegal actions, and exploitation of infrastructure dependencies (Kizza & Kizza, 2008, p. 181)". Login password is the most frequently used for access control. Extensive lists of default accounts and passwords are not hard to find by searching on the Web. Moreover, the easy passwords are sometimes overlooked or ignored by system administrators which might result in attaching passwords and gaining access to a host or service with the privileges of a current user (Kanellis, Kiountouzis, Kolokotronis, & Martakos, 2006).

Authentication and Multifaceted Authentication Systems

Authentication is used to secure the system at a higher level and is defined as "the process of verification of the identity of a party who generated some data and of the integrity of the data" (Kizza & Kizza, 2008, p. 191). The basic authentication procedures for resource protection are in two required configuration steps. The third step is an optional procedure that depends on the user's needs from the server.

1. Create a password file
2. Set the configuration to use this password file
3. Optionally, create a group file (Authentication, Authorization, and Access Control)

Moreover, the third party policy can benefit the systems by enforcing the access policy of defining the groups and roles within each group (Kanellis, Kiountouzis, Kolokotronis, & Martakos, 2006). While choosing an appropriate authentication mechanism, there are various issues needed to be considered: identities, credential management, identity flow, and browser type (Meier, Mackman, Dunner & Vasire, 2006).

Biometric Technology

Using biometrics for verification of identity has become a great phenomenon in our society. Reed (2003) stated that biometrics can be defined by the level of involvement the user needs to provide to be biometrically measured. The two categories of biometrics are passive and active. Examples of passive biometrics are face, voice, and gait which are seen as invasive to the user's privacy. Examples of active biometrics are fingerprint, hand geometry, retinal scanning, and Iris scanning which provide a high level of certainty attained as to the user's identity (Reid, 2003). In addition, to provide a higher level of security, two methods can be integrated with multiple biometric technologies into a system that include match-on-card technology and the

hazardous materials safety and security operation test (Rosenzweig, Kochems, & Schwartz, 2004).

Firewall

The purpose of firewall technology is to enforce some level of access control between the Internet security zones where the access control list provides the rules dictating how the traffic flows (Mason, 2007). To control the network security, firewall technology was classified into two categories: dynamic and statics. Static firewall implementation provides consistent security; while the dynamic firewall opens up the challenge of devising a mechanism for dynamic firewall configuration (Subramanian et. al., 2008). They continued by stating that it is common to allow access of resources such as web server by unknown sources in a traditional Internet Firewall scenario. Thereafter, a firewall should be configured to allow incoming traffic from and to known and reliable sources.

Threat Management

Kanellis, Kiountouzis, Kolokotronis, and Martakos (2006) suggested that "threat management is separated between on-site physical security threats, and Internet threats. Physical security threats exploit passwords, virus protection, removable media, and incident handling. Creating of passwords is an important task that often is given little thought, due to the increase of systems and accounts that require password protection…." (p. 233). Care should be taken to ensure that an individual's login consists of a password unique to only one account, continued Kanellis, et al (2006).

Other Related Studies

When the academia and corporate world woke up to the first personal computer (PC) virus in 1986 (Shih et. al., 2008) nobody notably thought the concept would become a major menace to the financial industry let alone health care, retail or government. Today the activities of virus and antivirus machines have become a multi-billion dollar industry. Writers of virus and antivirus programs are locked in juxtaposition like a game of chess to claim superiority over the craft. Sometime it crosses our minds to contemplate the adage "set a thief to catch a thief" meaning that some antivirus software writers may also be involved in writing virus software or at least are happy that virus programs are flourishing.

As if the menace of PC viruses was not enough discomfort, writers of virus program explored the concept of transferring their codes to mobile phones, and they succeeded. In May 2000, a rudimentary mobile phone virus (VBS.Telefonica) (Shih et. al., 2008) surfaced to the amazement of mobile phone users. To make matters worse, as mobile phones morphed into personal digital assistants (PDAs), complex data handling and communication devices called smart phones, a Windows Mobile O.S.-based virus was released in 2004 to infect these smart phones (Shih et. al., 2008). To complicate issues further, the implementation of Bluetooth short range wireless technology (widely welcomed by the mobile phone industry) opened up the ease of virus transfer (the Cabir virus) from Bluetooth enabled devices to other Bluetooth enable devices within range and over the airwaves.

The human unease elicited by computer viruses of all types is reminiscent of the prediction of Chinua Achebe's novels "*Things Fall Apart,*" 1958 and "*No Longer at Ease*," 1960 and his insistence that "mere anarchy is loosed upon the world." Also, T.S. Elliot's (1927) "Journey of the Magi" which carries the following sentence "no longer at ease" because the old dispensation has passed is a reminder that mobile phone and computer use is today fraught with fears that did not exist initially.

It is prudent to differentiate between ordinary mobile phones without the capability of data and text exchange (some still exist today) and smart phones, PDAs, with the capacity to rival desktop computers. These smart phones take, store pictures and transmit pictures, process financial information (a dangerous proposition), store hundreds of contact lists and vital records, interface with corporate databases, surf the internet, play games and music and carry a variety of software such as Word Mobile, Excel Mobile, Outllook etc. The growth of smart mobile phones compared to base phones reached 27,000.000 in 2004 and 130,000,000 in 2008 globally intoned Leavitt (2005). This astronomical growth carries

with it the concomitant problem of security from malware and viruses.

In surveying articles and research work on mobile phones virus security, Shih et. al. (2008) reference Zheng, et. al. (2006), Han and kamber (2001), and White et. al. (1999) in which they described two algorithmic approaches that prevent viruses from wreaking havoc on mobile phones. The two approaches to mobile phone virus containment are the "signature-based" and "behavior-based." To determine to presence of a virus using the signature-based approach requires that the attacking virus must have a known signature and byte sequence and therefore can be identified as preexisting in the virus database. On the other hand, the behavior-based approach differentiates between the execution pattern of a suspect virus or object and tags that object based on abnormal and erratic behavior. The behavior approach can identify new and unknown viruses and objects and classify them into potential virus and commence the process of quarantine before dissection of its signature and before a major damage is done to the system.

By 2009, the estimated number of cell phones was put at 2 billion globally. These cell phones are potential prey to 300 different viruses.

Mobile phones today are almost ubiquitous and integrated with home phones, computer-based digital mechanisms in automobiles, home security and the internet (Lewis, 2003) thus providing a recipe for communication and lifestyle interruption. This is a troubling scenario because if avid virus program crafters produce a dangerous code and run it successfully through the internet it may produce a devastating effect on business and government. The aforementioned scenario is further exacerbated by the proliferation of Bluetooth-based devices that provide easy access to the internet. Lewis (2003) sounded this idea as an alarm when he cautioned that the bad guys are planning to target your mobile smart phone, your wireless email and instant messaging device and may be even your home security system or your car.

In a study partly sponsored by the National Science Foundation of China, Zheng et. al. (2006) identified some smart phones viruses in their literature search. The viruses are Cabir, Commwarrior, Brador and Skull that infect smart phones through their "communication interfaces". They transmit data by GPRS, WiFi and Bluetooth. The conclusion is that virus spread can be controlled by reducing "coverage radius", signal strength, mobile phone user movement and "less distribution density of mobile phones."

The difficulty in protecting mobile phones and their networks from damaging virus activities stems from continuous proliferation of smart mobile phones and PDAs (Choi et.al. 2007) and also the lack of proper knowledge of the functions, capabilities, and use of smart mobile phone virus protection software technology (Howell, et.al. 2008). The vulnerability of smart mobile phones to virus and malware attacks continue to be disturbing because software to prevent such attack is not readily installed on smart mobile phones (Morales, et. al., 2006). To make matters worse, the Bluetooth short range wireless communication technology provides ample opportunity for writers of mobile phone virus programs to spread their creation and obtain both transient and static information, (Koong, 2008) from their victims.

3. PURPOSE OF THE STUDY

The purpose of this study was to determine if university students' general familiarity with mobile phone communication safety and security measures translates to practical usage of mobile phone communication safety and security measures. In other words, is there a significant relationship between students' general familiarity with mobile phone communication and safety security measures and actual usage and practice of these same measures?

4. METHODOLOGY

Selection of Participants and Data Collection

A total of 867 usable questionnaires were collected from 1,100 that were distributed in 2007 to a random sample of 20 of the 90

universities that are members of the National Universities Commission of Nigeria. The target respondents were college students. The surveys were sent as email attachments to enable participants to download and use mouse click to make their selections and return the instruments via email. Prior to full blown administration of the questionnaire, a 100-person pilot test was conducted to ensure that the statements were easy to understand.

Instrumentation

A 23-item Likert-type scale survey was developed to collect data for this study. The survey consisted of three sections. In the first section (Table 1 in the Appendix) students were asked to indicate on a three-point scale whether they are unfamiliar, somewhat familiar or extremely familiar with a given information security and safety measure. In the second section (Table 2) they were asked to indicate the percentage of times, <31%, 31-50%, and >50%, that they have used each security and safety measure in the past 12 months on their mobile phone communication devices. The third section (Table 3) requested some demographic data. The survey instrument was critiqued by other researchers for redundancy, ambiguity and readability of questions. This portion of the survey instrument is part of a larger study that encompasses four continents – Africa, Europe, China, and US. Experts who critiqued the instrument were also from Africa, U.S., and Europe.

Research Questions and Hypotheses

The statements in Tables 2 and 6 represent the eight research questions used to evaluate how the respondents actually use and put into practice mobile phone communication safety and security measures.

We proposed and tested the following eight hypotheses.

1. There is no significant relationship between **familiarity with** and actual **usage** of passwords as a security measure to protect mobile phone communication devices.
2. There is no significant relationship between **familiarity with** and actual **usage** of daily mobile phone communication system scan as safety and security measure.
3. There is no significant relationship between **familiarity with** and actual **usage** of mobile phone communication device system scan of email attachments as safety and security measure.
4. There is no significant relationship between **familiarity with** and actual **usage** of mobile phone communication device anti-virus software as safety and security measure.
5. There is no significant relationship between **familiarity with** and actual **usage and placement** of passwords on email attachments on mobile phone communication device.
6. There is no significant relationship between **familiarity with** and actual **usage** of biometric authentication on mobile phone communication device as safety and security measure.
7. There is no significant relationship between **familiarity with** and actual **usage** of firewalls on mobile phone communication device as safety and security measure.
8. There is no significant relationship between **familiarity with** and actual **usage** of multifaceted authentication systems on mobile phone communication device as safety and security measure.

Data Analysis

By utilizing the Statistical Package for the Social Sciences (SPSS) version 15.0, the collected data was analyzed with descriptive statistics, cross tabulations, linear regression, and analysis of variance (ANOVA). To avoid research bias, ANOVA with post hoc was also used to determine whether the statistically significant differences found between the independent and dependent variables (Field, 2000) were reliable. Table 4 presents the frequencies/percentages of general levels of familiarity (unfamiliar, somewhat familiar and extremely familiar) and percentages of usage (<31%, 31-50%, > 50%) of security

measures on mobile phone communication devices.

5. FINDINGS

Of the one thousand one hundred surveys that were distributed 867(79%) usable ones were returned. Demographic information are as follows: female (54%), undergraduate (63%), graduate (38%); majors in Arts & Sciences (29%), Business (37%), Engineering (18%), Others (16%); and level of experience in computing were Expert (46%), Very good (22%), Good (18%), Poor/Novice (14%). The following are relevant descriptions of each measure:

Demographic Results
The findings showed that a high percentage of participants spent a small amount of time to ensure the security of their mobile phone communication devices and information. A range of 43.8% to 53.5% of participants checked the least amount of time they practice using the following items: passwords usage, placement of passwords on email attachments, biometric authentication, firewalls, and multifaceted authentication systems. However, regarding scanning and antivirus protection, there were some good news to share: (a) 51.2% of participants spent more than 30% of their time to have their mobile phone communication devices scanned; (b) 41.5% of participants spent more than 30% of their time scanning email attachments on their mobile phone communication devices; and (c) 41.8% of participants made sure the antivirus software on their mobile phone communication devices was current.

Gender: Overall, there was no significant difference between the males and females' responses. However, the pattern we observed indicated that females spent less time than males for each item, except placement of passwords on email attachments on their mobile phone communication device before sending (see figure 1).

In addition, two items showed a significant difference between females and males: (a) Daily mobile phone communication devices scan (automated & manual) (t=-3.460, p<.01); and (b) How to ensure that firewalls on mobile phone communication devices are active (t=-2.901, p<.01). The linear regression results showed the same significant outcomes for those two items: the Beta value of .158 (p<.01) was for the first item and the Beta value of .117 (p<.01) was for the second item. The pattern in the findings indicated that males spent more time to ensure and scan their mobile devices than females.

Age: There was a significant difference between the age groups' responses. Based on the Tukey HSD results, the findings showed that the responses from the age group of greater than 50 years-old formed a significant subset group of people spending more time for all items, except how to ensure the viability of multifaceted authentication systems as security measure. The linear regression results showed four significant outcomes from those eight items (see Table 5).

Classifications: There was no significant difference between the graduate and undergraduate students' responses. However, the only one item that showed a significant difference (B= -.126, t=-3.506, p<.01) was that graduate students spent less time than the undergraduate students on "How to ensure that firewalls on mobile devices are active?" (see figure 2).

Major: There was a significant difference among the college major groups' responses. The findings showed that students of Arts and Science and College of Business spent less time on five of the eight mobile phone communication safety and security measures (see Figure 3). There were significant coefficients for all items, but two: "Scan of email attachments on your mobile phone communication device (automated and manual)" and "How to use biometric technology as security measure on mobile phone communication devices?."

Knowledge and experience with computers: There was a significant difference between the levels of knowledge and experience with computers and the participants' responses from four items: (a) Use of passwords to protect mobile phone communication device (B= -.069, t=-1.986, p=.047); (b) Scan of email attachments on your mobile phone communication device (automated and manual) (B= .178, t=4.36,

p<.01); (c) How to make sure the anti-virus software on your mobile phone communication device is current (B= -.130, t=-2.661, p<.01); and (d) How to place passwords on email attachments on your mobile device before sending (B= -.140, t=-4.049, p<.01).

Hours of waiting after mobile* phone communication *device malfunction: Again, there was a significant difference among the hours the participants waited after malfunction and the participants' responses from four items: (a) Use of passwords to protect mobile phone communication devices (B= -.078, t=-2.215, p=.027); (b) Scan of email attachments on your mobile phone communication device (automated and manual) (B= -.107, t=2.610, p<.01); (c) How to make sure the anti-virus software on your mobile phone communication device is current (B= -.143, t=-2.910, p<.01); and (d) How to use biometric authentication as security measure on mobile phone communication devices(B= -.150, t=-3.584, p<.01).
The observed pattern showed that the more hours of waiting after computer malfunction, the less time they spent on controlling information safety and security for their mobile devices.

Change Password Frequencies: The findings showed that there was no significant difference within the items. However, we observed a pattern which showed that the more frequent they changed their passwords, the less time they spent on controlling information safety and security on their mobile devices.

Levels of Familiarity and Usage of Mobile phone communication Security Measures
The following figures are paired graphical representations of levels of familiarity with and actual usage of mobile phone communication safety and security measures.

Passwords: Figure 4a illustrates that 87% of respondents are unfamiliar with passwords. Figure 4b shows that only a dismal 9% use passwords on their mobile phone communication devices more than 50 percent of the time. This is a deplorable statistic on such an important issue in information security. The non-deployment of passwords to protect mobile systems by a large number of students is a precarious contribution to the problem of system compromise. The same concern was echoed in a previous studies (Teer, Kruck, & Kruck, 2007) and (Aytes & Connolly, 2004) that did not provide accolades to students for their computing stance. However, based on the statistical analysis, there was no significant relationship between familiarity with and usage of passwords. This finding was of serious concern to us as researchers and educators. When you disregard the levels of familiarity with passwords and focus on actual usage which shows that more than 90% of participants did not practice using passwords to protect their systems you feel that digital education has to be reoriented.

Daily Computer System Scan: Figure 5a shows that 50% of respondents are unfamiliar with daily computer systems scan but 32% (a welcome number) use it on mobile devices more than 50% of the time. Because daily computing system scan is an automatic process in contemporary computing, most people may probably know that it is happening during the boot process and interpret that as using it. Therefore, the statistical results showed that there was no significant relationship between familiarity with and usage of daily computer system scan.

Scan of Email Attachments: Figures 6a and 6b indicate that 75% of respondents are unfamiliar with scan of email attachments while 26% use it more than 50% of the time. Again, since email scanning is generally an automatic process respondents may consider familiarity and usage to fall in the same realm of understanding and therefore claim usage. The statistical analysis showed that there was a significant relationship between familiarity with and usage of scan of email attachments. In other words, the more the participants are familiar with scanning of email attachments, the more time they spent on using and practicing this task.

Anti-virus software: Figures 7a and 7b indicate that 56% of respondents are unfamiliar with anti-virus software but only 27% use it more than 50% of the time. Most computer systems today have

preinstalled anti-virus software or have an online access to one and therefore usage may be automatic. The data that indicates that only 27% use it more than 50% of the time may be a reflection of those who do not have an online access to anti-virus software and therefore have to purchase and install their own copy. Our thought is that a higher percentage of students may have anti-virus software on their mobile devices. The statistical analysis showed that there was a significant relationship between familiarity with and usage of using anti-virus software. The more the participants are familiar with anti-virus software, the more time the participants spending on using anti-virus software.

Password on Email Attachments: Figure 8a shows that 79% of participants are unfamiliar with how to create a password, build it into a file and attach the file to email. Figure 8b indicates that using mobile devices, only 13% use passwords on email attachments more than 50% of the time. A-seventy nine percent unfamiliarity with password attachment and a dismal 13% usage for more than 50% of the time are deplorable for students. This finding is indicative of results from previous studies (Teer, Kruck, & Kruck, 2007) and (Aytes & Connolly, 2004) that show student indifference towards proper and safe computing. Therefore, the statistical results showed the same findings as the first studied item of passwords. There was no significant relationship between familiarity with and usage of password on email attachments.

Biometric Authentication: Figure 9a indicates that 94% of respondents are unfamiliar with biometric authentication while only 22% uses it more than 50% of the time on their mobile phone communication devices (Figure 9b). Since biometric authentication uses the uniqueness of what humanity already possesses such as finger printing or retinal scanning and we do not have to make an effort to remember anything such as passwords, it is a technology that should be required to interface between all systems users and systems. The statistical analysis showed that there was a significant relationship between familiarity with and usage of biometric authentication. The more the participants are familiar with biometric authentication issues, the more time they spent on this practice.

Firewalls: Figure 10a shows that 63% of respondents are unfamiliar with firewalls while only 5% use it on their mobile devices more than 50% of the time (Figure 10b). Firewalls filter incoming traffic before they arrive at the computer station or device and therefore their presence may not be apparent to the non-savvy user. When a user receives a server-notice of a virus-infected email that was blocked, it becomes apparent that a server firewall is at work. Therefore, the statistical results showed that there was no significant relationship between familiarity with and usage of firewalls.

Multifaceted Authentication Systems: Figure 11a shows that 94% of respondents are unfamiliar with multifaceted authentication systems while only 3% uses it more than 50% of the time. This unfamiliarity is not surprising because multifaceted authentication system is a higher order complex system protection apparatus designed for savvy computer users. Again, the statistical results showed that there was no significant relationship between familiarity with and usage of multifaceted authentication systems.

6. HYPOTHESES TESTED IN THIS STUDY

We did not find any empirical studies that looked at the relationship between students' familiarity with and usage of safety and security measures in the context of mobile phone communication devices. Researches that explored students' performance in the application of information security issues did not absolve students (Aytes and Connolly, 2004;Teer et.al., 2007). Given the literature search and our own experiences regarding security and safety of data on mobile devices in the U.S., China and Africa we tested the hypotheses below.

Table 6 shows the results of SPSS 15 cross tabulations and Chi-Squares of familiarity with and usage of mobile phone communication security and safety measures.

Hypothesis 1: Passwords. We found no significant relationship between familiarity with and usage of passwords at the .05 level thus supporting the null hypothesis.

Hypothesis 2: Daily computer systems scan. We found no significant relationship between familiarity with and usage of daily computer systems scan at the .05 level thus supporting the null hypothesis.

Hypothesis 3: Scan of email attachments. We found a significant relationship between familiarity with and usage of Scanning of email attachments at the .05 level, thus rejecting the null hypothesis.

Hypothesis 4: Anti-virus software. We found a significant relationship between familiarity with and usage of anti-virus software at the .05 level, thus rejecting the null hypothesis.

Hypothesis 5: Passwords on email attachments. We found no significant relationship between familiarity with and usage of scanning email attachments at the .05 level, thus supporting the null hypothesis.

Hypothesis 6: Biometric authentication. We found a significant relationship between familiarity with and usage of biometric authentication at the .05 level, thus supporting the null hypothesis.

Hypothesis 7: Firewalls. We found no significant relationship between familiarity with and usage of Firewalls at the .05 level, thus supporting the null hypothesis.

Hypothesis 8: Multifaceted authentication systems. We found no significant relationship between familiarity with and usage of multifaceted authentication systems at the .05 level, thus supporting the null hypothesis.

7. CONCLUSION

Five of eight hypotheses showed no significant relationship between familiarity with and actual usage of areas studied. This study showed an interesting profile related to the participants' mobile phone communication safety and security measures. We found that the primary factors that affect mobile phone communication security measures were as follows: (a) Age range, (b) Major, (c) Knowledge and experience with computers, and (d) Number of hours they spent waiting for their mobile phone device to be repaired after malfunction. The finding indicating that greater than 50 years-old respondents spent more time for all items may be a reflection of interest in harnessing the power of new technology. Arts and Science and College of Business students spent less time on five out of eight survey items. Moreover, the levels of knowledge and experience with computers showed a different degree of information technology safety and security measures. Thereafter, the number of hours respondents waited for their computer to be repaired after a malfunction were correlated with their knowledge and experience with computers.

Moreover, the following significant variables such as, scan of email attachments, anti-virus software, password on email attachments and biometric authentication show that familiarity with each of the variables does translate to usage. The level of knowledge and experience with computers is evidenced as the markup guideline for strengthening the mobile phone communication security and safety issues.

We therefore conclude that students who are familiar with the foregoing security measures are also practical users of these measures on mobile phone communication devices. This study guides us to focus on further issues of increasing familiarity with phone communication security and safety among college students. In addition, we are hoping that the results of this study will increase safety and security awareness and reduce negative economic impact and cyber-crime in African countries in the future.

8. Discussion

We found that it is vital to introduce the basic concepts of information security issues at an early stage of our prospective employees' lives. No nation should take the risks of weakening their sense of digital homeland security and suffer the socioeconomic impacts of cyber-crimes.

According to Ahamad, (2008), "Although we can argue that end users could do more to protect themselves and the online community, we should also expect more from the security industry in terms of viable solutions". He also supports a combination of security awareness, education, and personal responsibility in this digital life environment. We suggest that information security in mobile devices usage should be reinforced in the early stage of technological development in Nigeria.

9. Further Studies

This study can be replicated in the US and other countries. Considering the fact that safety and security of digital and non- digital data are uppermost in the minds of the world, we suggest this study be conducted among workers in corporate America.

10. REFERENCES

Africa Research Report. (2008). Retrieved January 18, 2009, from Internet World Stats: http://www.internetworldstats.com/africa2.htm

Achebe, Chinua (1958) Things Fall Apart, William Heinemann Ltd.

Achebe, Chinua (1960) No Longer At Ease, William Heinemann Ltd.

Ahamad, Mustaque (2008) Emerging cyber threads report for 2009. Georgia: Georgia Tech Information Security Center.

Authentication, Authorization, and Access Control (1996) Retrieved January 18, 2009, from Apache Http Server Project: http://httpd.apache.org/docs/1.3/howto/auth.html#basic

Aytes, Kregg and Terry Connolly (2004) "Computer security and risky computing practices: A rational choice perspective." Journal of Organizational and End User Computing, Volume 16, Number 3, pp. 22-40.

Choi, B. Young, Travice C. Bache, and Liza L. Hill (2007) "The pricing of wireless phone services in the USA: issues and development trends," *International Journal of Mobile Communications*, Volume 5, Number 2, pp. 169-185.

Eliot, S. Thomas (1927). *Journey of the Magi* published under Faber and Faber's series of Ariel Poems, 1927.

Field, Andy (2000) *Discovering statistics using SPSS for Windows.* Thousand Oaks, CA: Sage Publications.

Ghana Business News (GBN) (June 19, 2009) Nigeria mobile phone subscribers reach 68 million. Retrieved June 15, 2009. http://ghanabusinessnews.com/2009/06/19/nigeria-mobile-phone-subscribers-reach-68-million

Grabosky, Peter (2005) The global cyber-crime problem: The socio-economic impact. In R. Broadhurst & P. Grabosky, Cyber-Crime The Challenge in Asia, p. 43. Hong Kong: Hong Kong University Press.

Han, Jiawei and Micheline Kamber (2001) Data Mining Concepts and Techniques, Morgan Kaufman, PP. 284-287.

Howell, Mark; Steve Love and Mark Turner (2008) "User characteristics and performance with automated mobile phone systems," International Journal of Mobile Communications, Volume 6, Number 1, pp. 1-15.

Kanellis, Panagiotis; Evangelos Kiountouzis, Nicholas E. Kolokotronis, & Drakoulis Martakos (2006) Digital Crime and forensic science in cyberspace. Hershey, PA: Idea Group.

Kizza, J., & Florence M. Kizza (2008) Securing the information infrastructure. Hershey, PA: CyberTech.

Koong, S. Kai., Lai C. Liu, Shuming Bai and Bishan Lin (2008) "Identity Theft in the USA: evidence from 2002 to 2006," International Journal of Mobile Communications, Volume 6, Number 2, 199-216.

Kung, Lucy; Picard G. Roberts & Ruth Towse (2008) *The Internet and the Mass media.* Thousand Oaks, California: SAGE.

Leavitt, Neal (2005) "Mobile Phones, The Next Frontier for Hackers," *IEEE Computer, Volume* 38, Number 4, pp. 20-23.

Lewis, H. Peter (Dec. 2003) "The end of innocence in cell phones," *Fortune*, Volume 148, Number 12, pp. 68.

Mason, Andrew (2007) *Cisco Firewall Technology.* Indianapolis, Indiana: Cisco Press.

Meier, John; Alex Mackman; Michael Dunner, & Srinath Vasire (2006) Building Secure Microsoft ASP.NET Applications: Authentication, Authorization, and

Secure Communication. Redmond, Washington: Microsoft Press.

Morales, A. Jose; Peter J. Clarke; Yi Deng and Golam B. M. Kibria (2006) "Testing and evaluating virus detectors for handheld devices," *Journal in Computer Virology*, Volume 2, Number 2, pp. 135-147.

Okolo, Paul (June 19, 2009) Nigeria will Break Up Phone Company, Extends Deadline (Update2) http://www.bloomberg.com/apps/news?pid=20601116&sid=a8YcyXPyvuV0#. Retrieved June 30, 2009.

Ohuocha, Chijioke (2009) "Nigerian mobile market growing, revenues tailing off" from Reuters. http://www.reuters.com/article/rbssTechMediaTelecomNews/idUSLI3905120090618. Retrieved June 29, 2009.

Reid, Paul (2003) Biometrics for Network Security - Biometric technologies. Upper Saddle River, NJ: Pearson Education Inc.

Rosenzweig, Paul, Alane Kochems & Ari Schwartz (2004) Biometric Technologies: Security, Legal, and Policy Implications. Retrieved January 19, 2009, from The Heritage Foundation: http://www.heritage.org/Research/HomelandSecurity/lm12.cfm

Shifrin, Simon (2008) You have been hacked. The Idaho Business Review, Boise, June 30, 2008.

Shih, Dong-Her., Binshan Lin; Hsiu-Sen Chiang and Ming-Hung Shih (2008) "Security aspects of mobile phone virus: a critical survey." Industrial Management and Data Systems, Volume 8, number 4, 478-494.

Subramanian, N., Edara, U. R., & Ravi, K. B. (2008-08) DyNeF: Host-privilege-based dynamic network firewall for grid environment. World Academy of Science: Engineering & Technology, pp. 652.

Teer, P. Faye; S.E. Kruck and G.P. Kruck (2007) "Empirical Study of Students' Computer Security - Practices/Perceptions." Journal of Computer Information Systems, Volume 47, Number 3, pp. 105-110.

Water, Darren (2008) *Africa waiting for net revolution.* Retrieved January 18, 2009, from BBC News: http://news.bbc.co.uk/2/hi/technology/7063682.stm

White, R. Steve; Morton Swimmer; Edward J. Pring; William C. Arnold; David M. Chess, and John F. Morar (1999) "Anatomy of a Commercial Grade Immune System," IBM Research White Paper.

Wikipedia (2009). http://en.wikipedia.org/wiki/List_of_African_countries_by_population. Retrieved September 24, 2009.

Zheng, Hui., Dong Li and Zhuo Gao (2006) "An epidemic model of mobile phone virus," 2006 International Symposium on Pervasive Computing and Application," pp. 1-5. Network Research Center, Tsinghua University, P. R. China

APPENDIX

Table 1: FAMILIARITY AND CONFIDENCE WITH MOBILE PHONE SECURITY MEASURES

	Please circle your level of familiarity and confidence with the mobile phone security measures below.			
1	Level of familiarity with how to use passwords to protect your mobile phone communication device and data	Not Familiar	Somewhat Familiar	Extremely Familiar
2	Level of familiarity with daily mobile computer system scan	Not Familiar	Somewhat Familiar	Extremely Familiar
3	Level of familiarity with Scanning of email attachments on your mobile phone communication device	Not Familiar	Somewhat Familiar	Extremely Familiar
4	Level of familiarity with functions and usage of anti-virus software on mobile device	Not Familiar	Somewhat Familiar	Extremely Familiar
5	Level of familiarity with placements of passwords on email attachments on your mobile device before sending.	Not Familiar	Somewhat Familiar	Extremely Familiar
6	Level of familiarity with functions of biometric authentication as a security measure on mobile device	Not Familiar	Somewhat Familiar	Extremely Familiar
7	Level of familiarity with functions of firewalls on mobile device as security measures	Not Familiar	Somewhat Familiar	Extremely Familiar
8	Level of familiarity with functions of multifaceted authentication systems on mobile device	Not Familiar	Somewhat Familiar	Extremely Familiar

Table 2: REGULARITY OF USAGE AND PRACTICE OF MOBILE PHONE SECURITY MEASURES

	Indicate on average the percentage of times you have actually used or practiced the following measures when using mobile phones *in the past 12 months*			
1	Use of passwords to protect your mobile phone device and data	<=30%	31-50%	>50%
2	Daily mobile phone systems scan	<=30%	31-50%	>50%
3	Scan of email attachments on your mobile phone device (automated and manual)	<=30%	31-50%	>50%
4	How to make sure the anti-virus software on your mobile phone device is current.	<=30%	31-50%	>50%
5	How to place passwords on email attachments on your mobile phone device before sending.	<=30%	31-50%	>50%
6	Placements of passwords on email attachments before sending.	<=30%	31-50%	>50%
7	How to ensure that firewalls on mobile phone devices are active	<=30%	31-50%	>50%
8	How to ensure the viability of multifaceted authentication systems as security measures	<=30%	31-50%	>50%

Table 3: DEMOGRAPHICS

1	Gender	Female		Male		
2	Age range	18-25	26-30	31-45	46-50	>50
3	Classification	Undergrad		Graduate		
4	Major	Arts/Sciences		Business	Engineering	Other
5	Knowledge and Experience with mobile devices	Poor		Good	Very Good	Expert
6	Number of days you have waited in the past 12 months for your computer to be repaired after a malfunction.	< 1 day	1-3 days	4-7 days	8-14 days	>14 days
7	Number of times you have changed the password on your mobile device in 12 months?	0 times	1-4 times	5-10 times	11-30 times	>30 times

Table 4: Simple comparison of levels of familiarity with actual usage of mobile phone security measures

	Level of Familiarity			**Mobile Phone Security Measure (percent of the time used)**		
Security Measures	**Unfamiliar**	**Somewhat Familiar**	**Extremely Familiar**	**<31%**	**31-50%**	**>50%**
Use passwords	857(87%)	85(10%)	25(3%)	728(84%)	63(7%)	76(9%)
Daily computer system scan	432(50%)	164(19%)	271(31%)	423(49%)	167(19%)	277(32%)
Scan of email attachments	651(75%)	79(9%)	137(16%)	507(59%)	131(15%)	229(26%)
Anti-virus software	484(56%)	171(20%)	212(25%)	418(48%)	216(25%)	233(27%)
Password on email attachments	682(79%)	79(9%)	106(12%)	679(78%)	74(9%)	104(13%)
Biometric authentication	819(95%)	38(4%)	10(1%)	563(65%)	116(13%)	188(22%)
Firewalls	544(63%)	184(21%)	139(16%)	699(81%)	123(14%)	45(5%)
Multifaceted authentication systems	818(94%)	41(5%)	8(1%)	784(90%)	58(7%)	25(3%)

Table 5: Linear Coefficients for the Variable of Age Item

Survey Item	***Beta***	***t***
How to make sure the anti-virus software on your mobile phone device is current.	-.260	.01 *
How to place passwords on email attachments on your mobile phone device before sending	.086	.01 *
How to use biometric technology as security measure on mobile phone devices	.227	.01 *
How to ensure that firewalls on mobile phone devices are active	.141	.01 *

Note: * The significant value is less than .001.

Table 6: Cross Tabulations and Chi-Squares Analyses of **Familiarity with** and **Usage** of Mobile Phone Security and Safety Measures

	Familiarity versus Usage	Chi-Square Value	df	Significant at .05
$H_0$1	Passwords	15.595	4	.265
$H_0$2	Daily computer system scan	94.466	4	.179
$H_0$3	Scan of email attachments	128.866	4	.000*
$H_0$4	Anti-virus software	181.386	4	.000*
$H_0$5	Passwords on email attachments	32.859	4	.024
$H_0$6	Biometric authentication	41.350	4	.000*
$H_0$7	Firewalls	28.048	4	.782
$H_0$8	Multifaceted authentication systems	12.982	4	.957

*Significance at p<.05

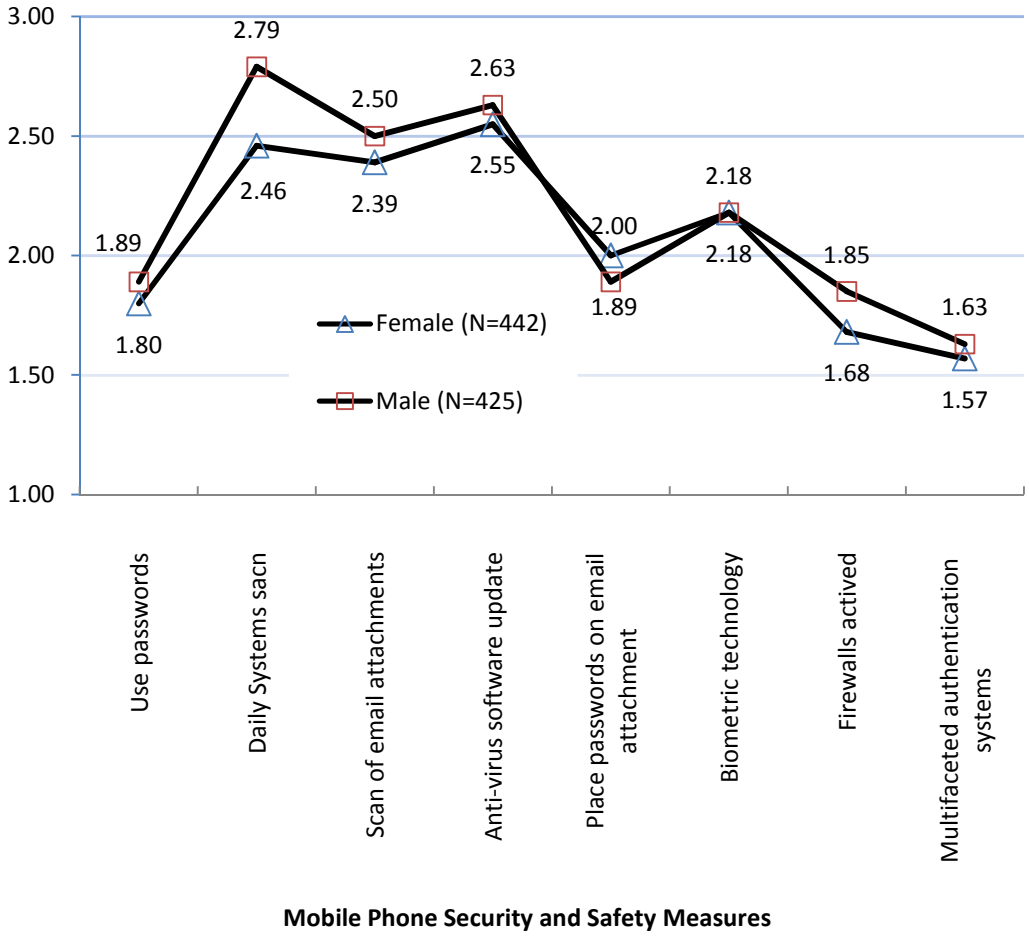


Figure 1: Mean value of gender responses

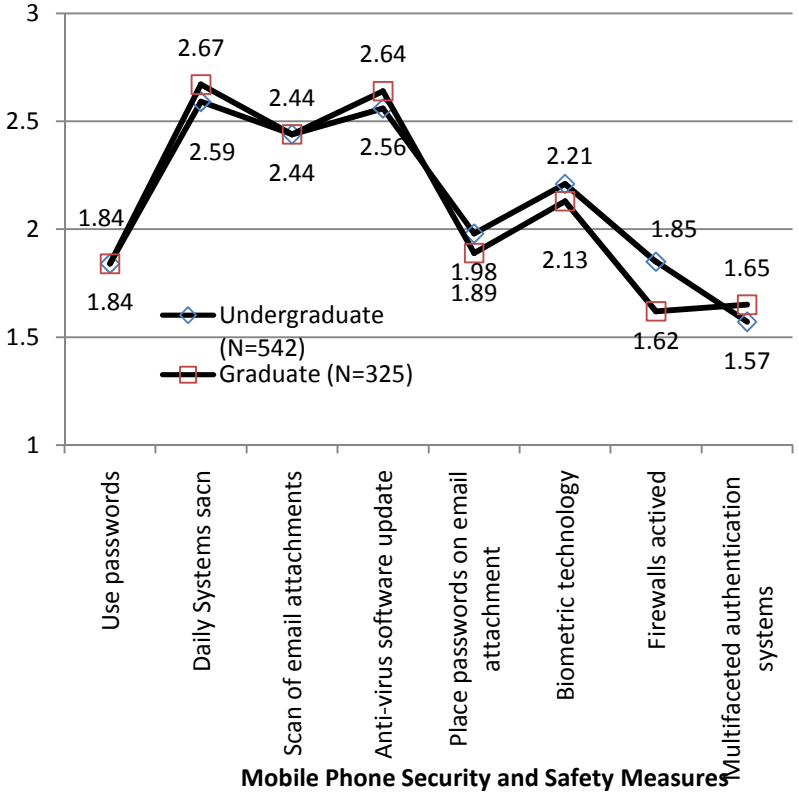


Figure 2: Mean value of responses from Classification

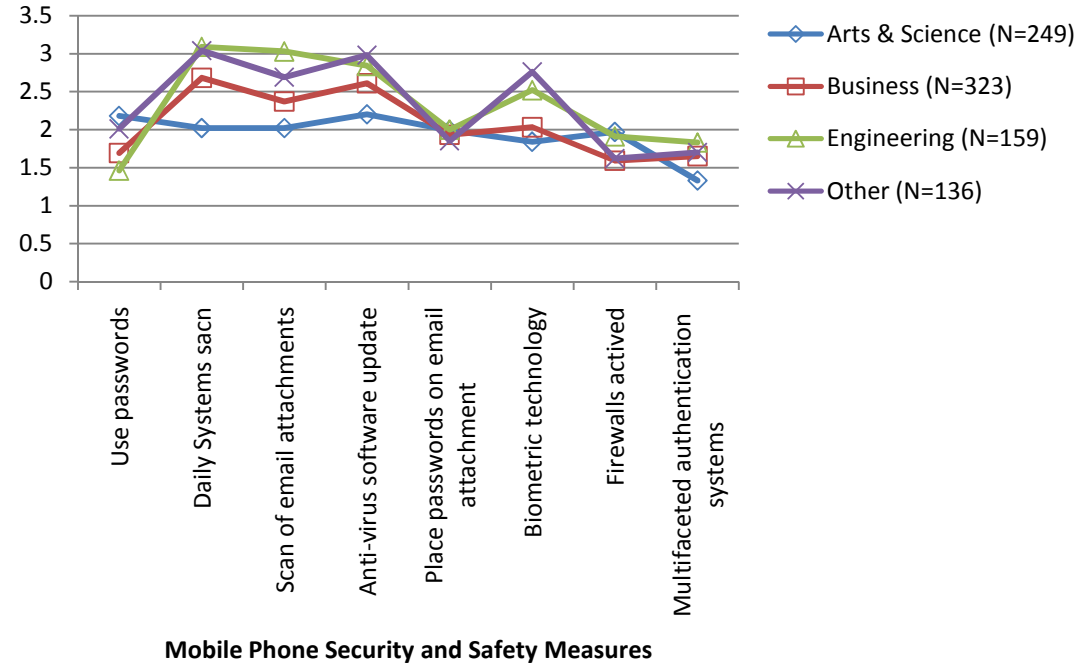
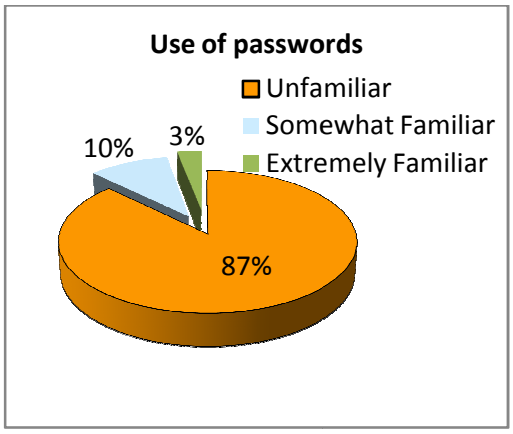
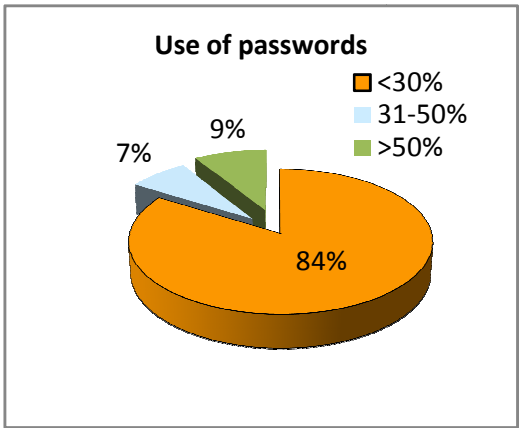
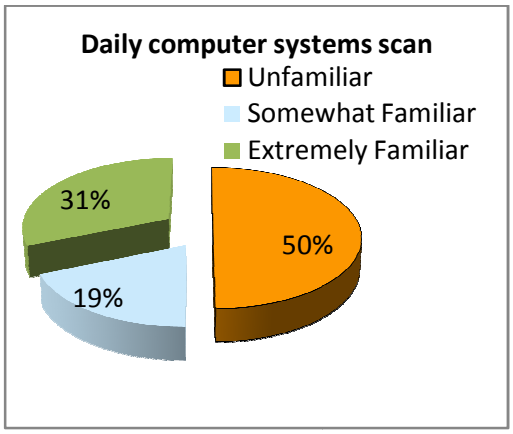


Figure 3: Mean value of responses from Majors





Figures 4a&b. Familiarity with passwords (4a) and Usage of passwords (4b)



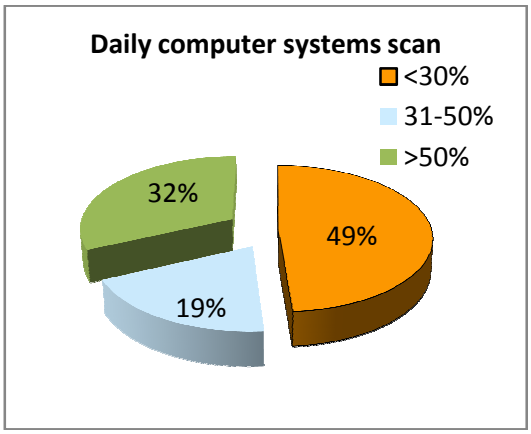
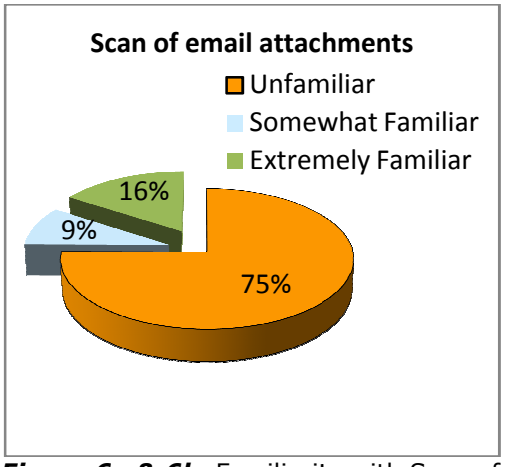


Figure 5a & 5b. Familiarity with Daily mobile computer systems scan (5a) and Usage of Daily mobile computer systems scan (5b)



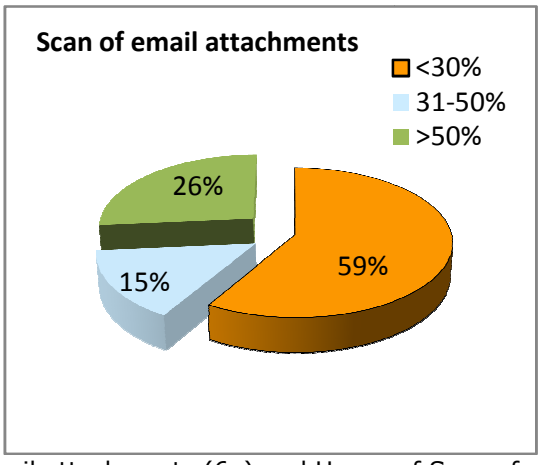


Figure 6a & 6b. Familiarity with Scan of email attachments (6a) and Usage of Scan of email attachments (6b)

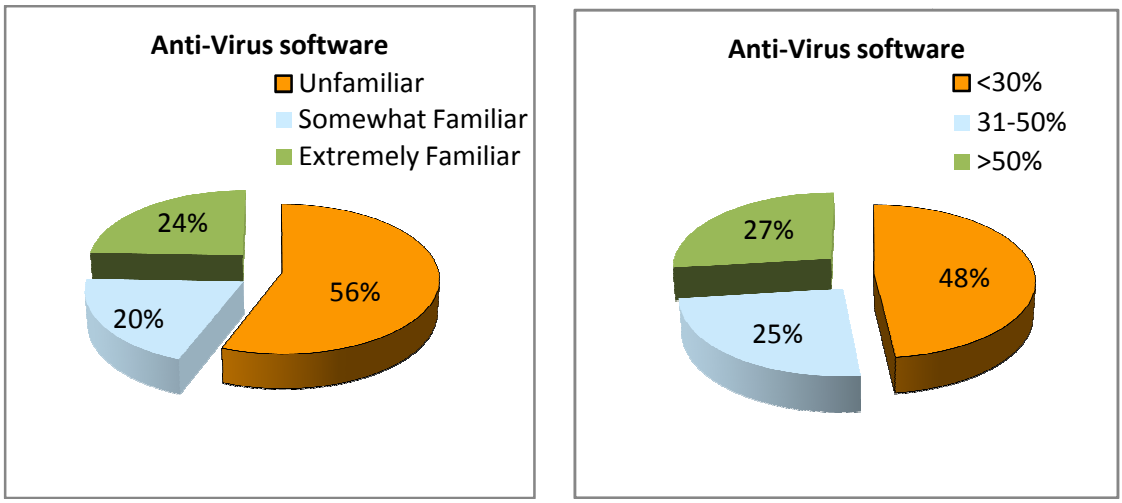


Figure 7a & 7b. Familiarity with anti-virus software (7a) and Usage of the anti-virus software (7b)

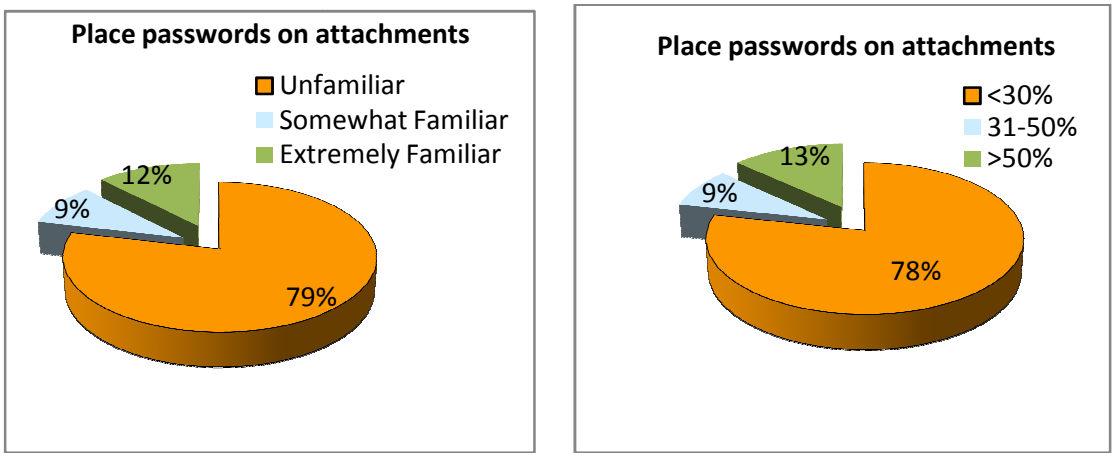


Figure 8a & 8b. Familiarity with email attachments (8a) and Usage of how to place passwords on email attachments (8b)

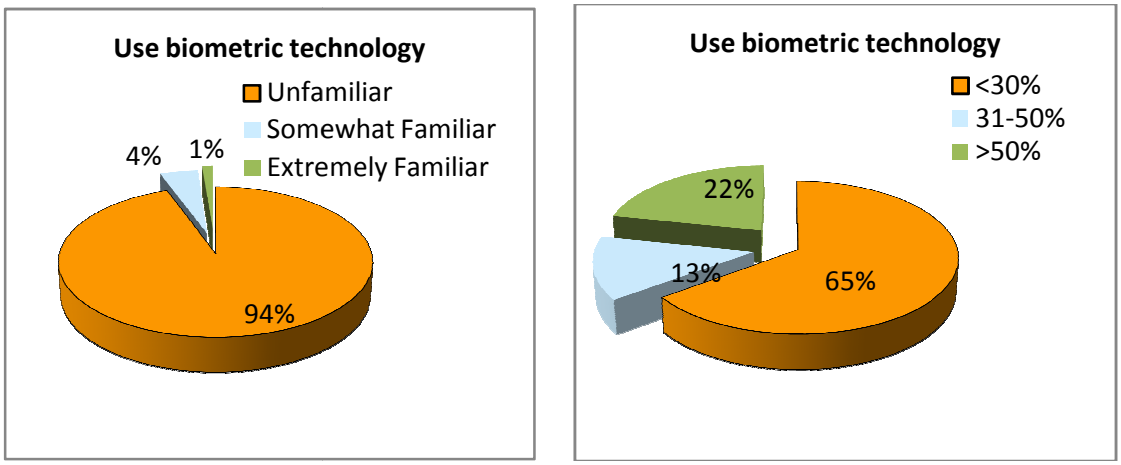


Figure 9a & 9b. Familiarity with biometric technology (9a) and Usage of biometric technology (9b)

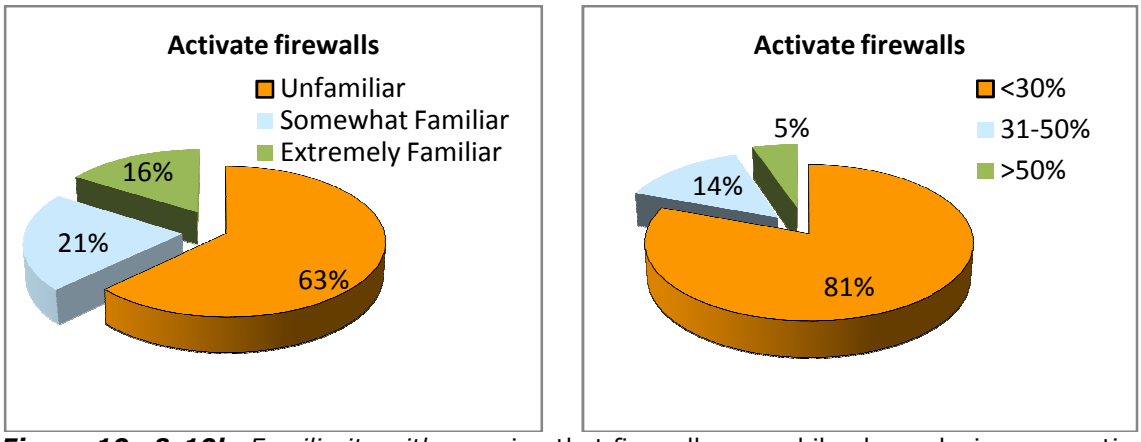


Figure 10a & 10b. *Familiarity with* ensuring that firewalls on mobile phone devices are active (10a) and *Usage of h*ow to ensure that firewalls on mobile phone devices are active (10b)

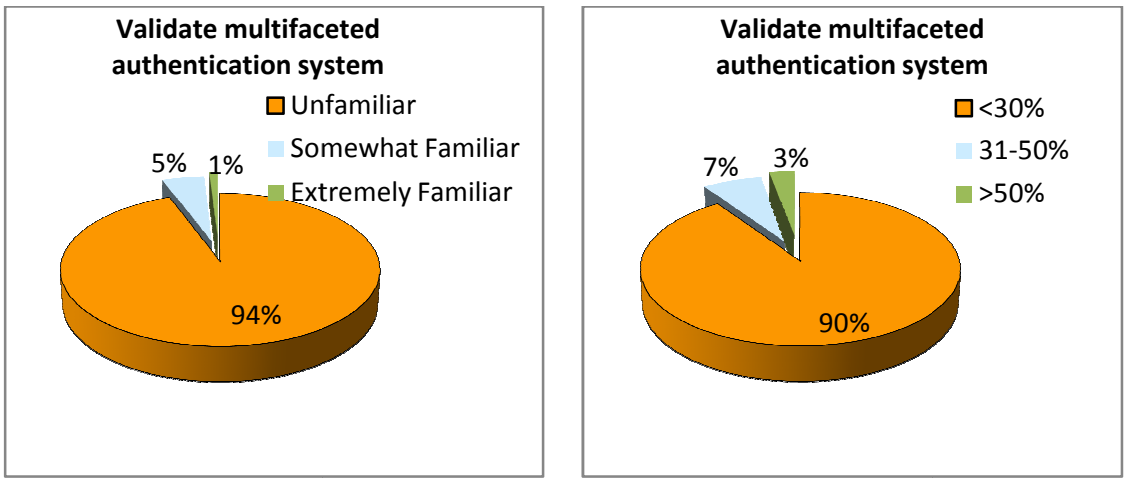


Figure 11a & 11b. Familiarity with how to ensure the viability of multifaceted authentication systems as security measures (11a) and usage of how to ensure the viability of multifaceted authentication systems as security measures (11b)