INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

IJRCM

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A., Google Scholar, Indian Citation Index (ICI), Open J-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)], Index Copernicus Publishers Panel, Poland with IC Value of 5.09 (2012) & number of libraries all around the world.

Circulated all over the world & Google has verified that scholars of more than **5771 Cities** in **192 countries/territories** are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

http://ijrcm.org.in/

CONTENTS

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to the recent developments & practices in the areas of Computer Science & Applications; Commerce; Business; Finance; Marketing; Human Resource Management; General Management; Banking; Economics; Tourism Administration & Management; Education; Law; Library & Information Science; Defence & Strategic Studies; Electronic Science; Corporate Governance; Industrial Relations; and emerging paradigms in allied subjects like Accounting; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Rural Economics; Co-operation; Demography: Development Planning; Development Studies; Applied Economics; Development Economics; Business Economics; Monetary Policy; Public Policy Economics; Real Estate; Regional Economics; Political Science; Continuing Education; Labour Welfare; Philosophy; Psychology; Sociology; Tax Accounting; Advertising & Promotion Management; Management Information Systems (MIS); Business Law; Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labour Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; International Relations; Human Rights & Duties; Public Administration; Population Studies; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism & Hospitality; Transportation Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic; Web Design and emerging paradigms in allied subjects.

Anybody can submit the **soft copy** of unpublished novel; original; empirical and high quality **research work/manuscript** ***anytime*** in ***M.S. Word format*** after preparing the same as per our **GUIDELINES FOR SUBMISSION**; at our email address i.e. infoijrcm@gmail.com or online by clicking the link **online submission** as given on our website (***FOR ONLINE SUBMISSION, CLICK HERE***).

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____

THE EDITOR

IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF _____.**

(e.g. Finance/Mkt./HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript titled '_____' for likely publication in one of your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published anywhere in any language fully or partly, nor it is under review for publication elsewhere.

I affirm that all the co-authors of this manuscript have seen the submitted version of the manuscript and have agreed to inclusion of their names as co-authors.

Also, if my/our manuscript is accepted, I agree to comply with the formalities as given on the website of the journal. The Journal has discretion to publish our contribution in any of its journals.

NAME OF CORRESPONDING AUTHOR	:
Designation/Post*	:
Institution/College/University with full address & Pin Code	:
Residential address with Pin Code	:
Mobile Number (s) with country ISD code	:
Is WhatsApp or Viber active on your above noted Mobile Number (Yes/No)	:
Landline Number (s) with country ISD code	:
E-mail Address	:
Alternate E-mail Address	:
Nationality	:

* i.e. Alumnus (Male Alumni), Alumna (Female Alumni), Student, Research Scholar (M. Phil), Research Scholar (Ph. D.), JRF, Research Assistant, Assistant Lecturer, Lecturer, Senior Lecturer, Junior Assistant Professor, Assistant Professor, Senior Assistant Professor, Co-ordinator, Reader, Associate Professor, Professor, Head, Vice-Principal, Dy. Director, Principal, Director, Dean, President, Vice Chancellor, Industry Designation **etc**. ***The qualification of author is not acceptable for the purpose***.

NOTES:

a) The whole manuscript has to be in ***ONE MS WORD FILE*** only, which will start from the covering letter, inside the manuscript. ***pdf. version is liable to be rejected without any consideration***.

b) The sender is required to mention the following in the **SUBJECT COLUMN of the mail**:

New Manuscript for Review in the area of (e.g. Finance/Marketing/HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

c) There is no need to give any text in the body of the mail, except the cases where the author wishes to give any **specific message** w.r.t. to the manuscript.

d) The total size of the file containing the manuscript is expected to be below **1000 KB**.

e) Only the **Abstract will not be considered for review** and the author is required to submit the **complete manuscript** in the first instance.

f) ***The journal gives acknowledgement w.r.t. the receipt of every email within twenty-four hours*** and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of the manuscript, within two days of its submission, the corresponding author is required to demand for the same by sending a separate mail to the journal.

g) The author (s) name or details should not appear anywhere on the body of the manuscript, except on the covering letter and the cover page of the manuscript, in the manner as mentioned in the guidelines.

2. **MANUSCRIPT TITLE:** The title of the paper should be typed in **bold letters**, **centered** and **fully capitalised**.

3. **AUTHOR NAME (S) & AFFILIATIONS:** Author (s) **name**, **designation**, **affiliation** (s), **address**, **mobile/landline number** (s), and **email/alternate email address** should be given underneath the title.

4. **ACKNOWLEDGMENTS:** Acknowledgements can be given to reviewers, guides, funding institutions, etc., if any.

5. **ABSTRACT:** Abstract should be in **fully Italic printing**, ranging between **150** to **300 words**. The abstract must be informative and elucidating the background, aims, methods, results & conclusion in a **SINGLE PARA**. ***Abbreviations must be mentioned in full***.

6. **KEYWORDS:** Abstract must be followed by a list of keywords, subject to the maximum of **five**. These should be arranged in alphabetic order separated by commas and full stop at the end. All words of the keywords, including the first one should be in small letters, except special words e.g. name of the Countries, abbreviations etc.

7. **JEL CODE:** Provide the appropriate Journal of Economic Literature Classification System code (s). JEL codes are available at www.aea-web.org/econlit/jelCodes.php. However, mentioning of JEL Code is not mandatory.

8. **MANUSCRIPT:** Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. *It should be free from any errors i.e.* ***grammatical***, ***spelling*** *or* ***punctuation.*** *It must be thoroughly edited at your end*.

9. **HEADINGS:** All the headings must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

10. **SUB-HEADINGS:** All the sub-headings must be bold-faced, aligned left and fully capitalised.

11. **MAIN TEXT:**

THE MAIN TEXT SHOULD FOLLOW THE FOLLOWING SEQUENCE:

INTRODUCTION

REVIEW OF LITERATURE

NEED/IMPORTANCE OF THE STUDY

STATEMENT OF THE PROBLEM

OBJECTIVES

HYPOTHESIS (ES)

RESEARCH METHODOLOGY

RESULTS & DISCUSSION

FINDINGS

RECOMMENDATIONS/SUGGESTIONS

CONCLUSIONS

LIMITATIONS

SCOPE FOR FURTHER RESEARCH

REFERENCES

APPENDIX/ANNEXURE

The manuscript should preferably be in ***2000 to 5000 WORDS***, But the limits can vary depending on the nature of the manuscript.

12. **FIGURES & TABLES:** These should be simple, crystal **CLEAR**, **centered**, **separately numbered** & self-explained, and the **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. *It should be ensured that the tables/figures are referred to from the main text*.

13. **EQUATIONS/FORMULAE:** These should be consecutively numbered in parenthesis, left aligned with equation/formulae number placed at the right. The equation editor provided with standard versions of Microsoft Word may be utilised. If any other equation editor is utilised, author must confirm that these equations may be viewed and edited in versions of Microsoft Office that does not have the editor.

14. **ACRONYMS:** These should not be used in the abstract. The use of acronyms is elsewhere is acceptable. Acronyms should be defined on its first use in each section e.g. Reserve Bank of India (RBI). Acronyms should be redefined on first use in subsequent sections.

15. **REFERENCES:** The list of all references should be alphabetically arranged. ***The author (s) should mention only the actually utilised references in the preparation of manuscript*** and they may follow Harvard Style of Referencing. **Also check to ensure that everything that you are including in the reference section is duly cited in the paper**. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc., in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italic printing. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parenthesis.
- ***Headers, footers, endnotes*** *and* ***footnotes*** *should* ***not be used*** *in the document.* However, **you can mention short notes to elucidate some specific point**, which may be placed in number orders before the references.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–23

UNPUBLISHED DISSERTATIONS

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

USERS' CONSCIOUSNESS AND PRACTICES REGARDING SMARTPHONE SECURITY THREATS, VULNERABILITIES AND SECURITY MEASURES: A RESEARCH IN THE TARKWA-NSUAEM MUNICIPALITY OF THE WESTERN REGION, GHANA

MAHENDRA KUMAR SHRIVAS
LECTURER & SYSTEM ADMINISTRATOR
ACADEMIC CITY COLLEGE
ACCRA

SAMUEL ANYIMAH
ICT & MATHEMATICS TUTOR
HUNI-VALLEY SENIOR HIGH SCHOOL
HUNI-VALLEY

JAMES BADU
LECTURER
ACADEMIC CITY COLLEGE
KUMASI

Dr. THOMAS YEBOAH
HEAD
DEPARTMENT OF ICT
CHRISTIAN SERVICE UNIVERSITY COLLEGE
KUMASI

ABSTRACT

Mobile phone; which in some few years past was nothing more than a call-making tool, and at best for text messaging, has evolved to be very powerful device, hence the modern name: Smartphone. Smartphone's unique computing capabilities, varied catalogue of software applications, fast connectivity, intuitive tendency and user-friendliness, blended with portability make it a fully-fledged miniaturized computer that fit into the user's pocket. Owing to the enormous functionalities and wealthy information a smartphone can hold, it has become an attractive mine field for attackers and malware creators. As smartphone gain unprecedented admiration and international usage statistics swells exponentially, hackers are enticingly lured to maliciously prey on the unsecured device of the uninformed user. This research focuses on smartphone user's consciousness towards mobile security threats, vulnerabilities and user's security culture and countermeasures taken to avert any mobile threat. The interpretation of results revealed that most of the smartphone users were not conscious of the need for security on their mobile handset nor do users enable the necessary security features.

KEYWORDS

mobile, smartphone, cyber security, vulnerabilities, countermeasures, mobile security, security threats.

I. INTRODUCTION

A. DEFINITION OF SMARTPHONE

Smartphone refers to the state-of-the-art cell phone device, distinguishable from the ordinary telephone by the integration of advanced features such as operating system to run software applications, wireless technology for connectivity, web browsers for internet accessibility, digital camera with video capturing capabilities and an embedded memory for storage [1].

Smartphone as "a mobile communication device is optimized in its specification and features to support one or more primary functions like music, video, gaming, pictures, browsing, mobile TV, navigation and messaging." Smartphones typically have larger displays, powerful processors, embedded memory, improved battery capacity and touchscreen for content manipulation and data input [2].

Smartphone is currently a fully-fledged miniaturized computer that fit into the user's pocket. Intended for making voice and video calls, web browsing, capturing videos and images, instant text messaging, playing built-in and downloaded games, listening to audio and watching videos, managing contacts, rendering social media applications, connecting to other devices via Bluetooth technology, mobile banking, storing personal data and a host of functionalities; smartphone has almost turned out to be an inseparable part of user's personal and professional lifestyle. It is becoming an intimate component of the digital ecosystem and has permeated the facets of modern lifestyle for millions of users around the world. Contemporary smartphones have improved capabilities, enhanced processing power, and unprecedented internet connectivity that make them to be virtually as resourceful as a computer [3].

Nevertheless, smartphones are open to security risk and security challenges that would yield undesirable results if left unattended to [4]. Hostile intruders and interlopers are relentlessly intercepting the device to gain access to sensitive information such as ATM codes, credit card pins, bank account numbers, login credentials, etc., that can lead them to steal elements of financial worth.

Furthermore, the smartness of the smartphone is displayed by the mobile applications it runs. These mobile applications have some mischievous ones which have malware embedded in it to spy on the user's call logs, browsing history, precise locations, and viewing private pictures or videos of victim's device.

There is therefore a need for defensive mechanisms to mitigate information leakage and data lost, protect the confidentiality and integrity of data, thwart the effort of ruthless spies from locating mobile devices, block unscrupulous intruders from accessing a locked phone, fish out malicious websites and emails, and remotely lock out phone thieves from cracking down the device for unsolicited information.

B. OBJECTIVES OF THE STUDY

The objective of this research is to evaluate user's awareness regarding smartphone security threats, vulnerabilities and to also appraise the countermeasures users take in the incidence of security threats. The specific objectives are:

1. To evaluate user's knowledge of smartphones security threats and vulnerabilities.
2. To analyze user's security culture and practices in the incidence of the security threat.

3. To propose efficient measures to protect the mobile device and its sensitive content

C. RESEARCH QUESTIONS

In realizing the purpose of the research, the following research questions are raised:

1. What is the level of importance that user's accord to the content or information stored of their smartphone?
2. Do smartphone users put in place authentication mechanisms or access control methods to restrict unauthorized access to their device?
3. Do smartphone users fully read and understand permissions that accompany mobile applications they download from the various mobile app stores?
4. Do smartphone users install security software on their device to detect, protect and offset any security threat?
5. Do smartphone users know the availability of anti-theft applications, locating tracking services or retrieval mechanisms that can be used to trail, wipe remotely or retrieve the device in case phone lost or theft?

D. IMPORTANCE OF THE STUDY

With virtually all financial businesses going mobile, social media applications via mobile device gaining unprecedented admiration, worldwide smartphone usage statistics swelling exponentially and hackers' skills growing to be more advanced, it is even more critical that mobile devices are appropriately provided the requisite security. Nearly every smartphone user stands a chance of being a prey of the malicious deeds of cybercriminals; consequently, the need for mobile security [5]. Keeping the user out of the darkness of ignorance of mobile security and enhancing the user's knowledge on mobile device security measures can greatly improve the compliance with effectual security practices to counterbalance any security threat to mobile devices [6].

II. RESEARCH REVIEW

A. MOBILE SECURITY THREATS AND CLASSIFICATION

Mobile security threat is a probable risk that might exploit a weakness in a system to violate security and consequently cause a possible mischief. The essential attractive entities for attackers of mobile devices are: the data on the device, the identity of users and the denial of service to user. [7]

Mobile security threats can be broadly classified as:

1. User-based threat vector
2. Application-based threat vector
3. Web-based threat vector
4. Network-based threat vector
5. Physical threat vector

User-based threat vector: The principal threat to the leakage of confidential and delicate material (images, videos, audio, etc.) on smartphones stems from user's sheer negligence and carelessness, rather than technical interloping [8]. Most users make their device an easy prey for attackers in their indulgence of unsafe behaviors such as not protecting the mobile device from unauthorized entry through access control mechanism (password, pattern or pin), ignorantly clicking on any link inserted in text messages or email from unknown sources, joining anonymous Wi-Fi networks and using free public Wi-Fi hotspots, not being particular about apps' permissions when installing apps and removing software restrictions on smartphone to evade security controls (Jail breaking or rooting). [9]

Application-Based Threat Vector: This threat resides in downloaded applications from mischievous websites or app stores. Some developers embed malicious codes into applications to fraudulently spy on users. Included in application-based threats are malware and spyware. *Malware* (shortened form of "Malicious software") executes its intended actions secretly while installed on smartphone without the user's awareness. It's mostly found in game demos and free apps. [10, 11]. *Spyware* is related to software that pops up advertisements (called *adware*) to generate a revenue pond for its creator. Information often aimed at by spyware includes call log history, received or sent text messages, user's precise location, browsing history, phonebook contact list, email's inbox or outbox. [12,13]. Recent report from Snoop Wall Mobile Security indicated that most flashlights on the Google Play Store are malicious and can access user's device storage and install additional backdoors or Remote Access Trojans (RATs). [14]

Web-based threat vector: This threat presents an incessant, relentless and persistent risk to mobile devices due to the fact that the device is continuously connected to the web. Some well-known major threats to smartphone via the web include: Phishing Scams (use of email or SMS to send illicit link, premeditated to trick receivers in given out passwords, pins, or useful information), Browser exploits [15] and Drive-By downloads (a misleading pop-up) [16] [17].

Network-based Threat Vector: Characteristically, smartphone supports cellular network (GSM) as well as local wireless networks (Wi-Fi and Bluetooth). These data transmission networks can horde various classes of threats such as Network exploits, Wi-Fi Sniffing [18] and Bluetooth network vulnerability [19] [20].

Physical Threat Vector: Possibly, the very lightness and portability of mobile phones makes them easily to be stolen or misplaced. This is the physical threat to the device. Stolen or misplaced smartphone also implies stolen or loss of sensitive data and information stored on the device. It is riskier, if the stolen or misplaced mobile device finds itself in the hands of an advanced attacker; slack security features of most mobile phones could be overpowered affording the attacker entry to any information stored [21] [22].

B. MOBILE SECURITY MEASURES

The risk of intruders interfering with mobile devices can be significantly reduced to barest minimum, if users are cautious to develop a security culture and apply proper security measures on their smartphones. Keeping the user out of the darkness of ignorance of mobile security and enhancing the user's knowledge through enlightenment can greatly improve the compliance with effectual security practices to counterbalance any security threat to mobile devices. The following tips can ensure maximum security on the device [23].

1. Securely lock mobile device with a PIN, pattern or password and set up a lock on the SIM card as well.
2. Install applications from only trusted app stores and toggle off the installation of application from "unknown sources" option in the security application settings menu.
3. Do not jailbreak, root or meddle with the mobile device software to evade its controls.
4. Remember to logout from websites initially signed in to transact business, shopping, or emailing services that requires user account.
5. Turn off Wi-Fi and Bluetooth when not in use. Also, do not transact business or shop online via free unsecured public Wi-Fi network.
6. Don't click on links or open attachments in emails or text messages from unknown and unsolicited sources.
7. Install mobile security software such as antivirus, spam filters and antispyware to safely protect the mobile device from the looming dangers of malware and spyware.

C. COUNTERMEASURES

A Countermeasure is an act, practice, or technique taken to neutralize the effect of a dangerous action. Generally used in Intrusion Prevention System (IPS), a "countermeasure is a defensive technology method used to prevent an exploit from successfully occurring once a threat has been detected" [24]. For maximum mobile security, the following countermeasures; which are also defense mechanisms should be adhered to. These include: countermeasures against misplaced or theft of mobile devices, countermeasures against malware infection and countermeasures against leakage of sensitive information [25]. These countermeasures are required to be proactive (i.e. putting up the necessary security measures in readiness for the risky action rather than waiting for the occurrence of the menace before acting.) or must be swift in response (i.e. the rapidness in reacting to a situation. In the occurrence of stolen phone, the victim must immediately go online and activate the anti-theft app or location tracking app installed on the phone). Some of the correct proactive and swift precautions may include:

a) Setting up a strong screen lock password to restrict unauthorized access [26].
b) Installation of Anti-theft and Lock Screen Protection Applications such as Lookout, Prey, Android Device Manager, Find My iPhone, Cerberus, etc. to locate misplaced or stolen device [27] [28].
c) Attachment of Owner's Information and activation of "the intelligent assistant" Siri on iPhone to assist in the returning of the device by an honest person who finds a misplaced device [29].
d) Keeping safely the smartphone's unique numbers: IMEI, serial number and model number for tracking and identification [30].

e) Installation of antivirus or anti-malware application to scan the device and fish out duplicitous software that may be inadvertently downloaded and installed on the handset.
f) Being cautious of repackaged and fake applications that mimic the original but are more likely to be malware or trojanized [31] [32]. A recent fake app, supposedly to be an antivirus, was "Virus Shield" misled a lot of users due to its professional appearance [33] and Flappy Bird; a favorite android game was feigned, trojanized and introduced to the app stores [34].
g) Patronizing the trusted app stores over third-party app stores [35].
h) Cautiously reading and comprehending app permissions, terms and conditions, end users license agreement and user's reviews and ratings before down-loading any app. [36].
i) Patronizing paid applications over supposedly free applications. Free applications appear harmless, but it could be a source of danger to user's privacy [37]. The ancient adage that "there's no such thing as a free lunch" seem to hold an element of truth. "If you are not paying for it, you're not the customer; you're the product being sold" [38]. Patronizing paid applications may reduce the lurking attack on user's information

III. RESEARCH METHODOLOGY

The research design used was both Quantitative and Qualitative Research inclined, which commenced by appraising related works and literature from journals, books, website, and reports. The quantitative phase was used in the data collection method, i.e. the use of questionnaire. The qualitative aspect was concerned with the subjective evaluation of respondent opinions to gain an essential understanding of the subject researched on.

The target population for this research was users of android and iOS powered smartphones within the Tarkwa-Nsuaem Municipal Assembly of the Western Region, Ghana.

Purposive or deliberate convenient sampling procedure was used for the research. This type of sampling technique involves a deliberate selection of particular components of the total population to represent the whole population, and inference and judgement made characterizes the whole. It is tagged convenient due to the ease of access during the selection.

The sample was 809 respondents of the 31,890 population who owned a mobile phone [39]. The sample was arrived at and adjusted from online sample size calculator with confidence level of 95% [40].

Data gathered from respondents was analyzed by using Microsoft Office Excel 2010. Pie charts and Bar graphs were used to graphically represent the data for easy judgement.

IV. RESULT ANALYSIS

FIGURE 1: BRAND OF SMARTPHONES USED BY RESPONDENTS

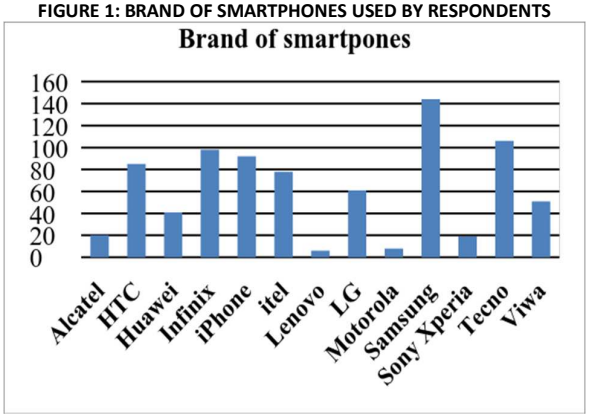


FIGURE 2: OPERATING SYSTEMS OF SMARTPHONES USED BY RESPONDENTS

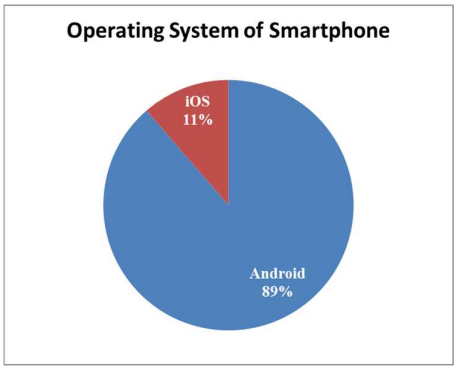


FIGURE 3: LEVEL OF IMPORTANCE OF INFORMATION ON RESPONDENT'S MOBILE DEVICE

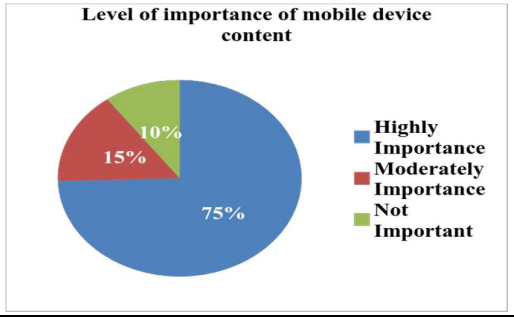


FIGURE 4: SCREEN LOCK METHODS USED BY RESPONDENTS

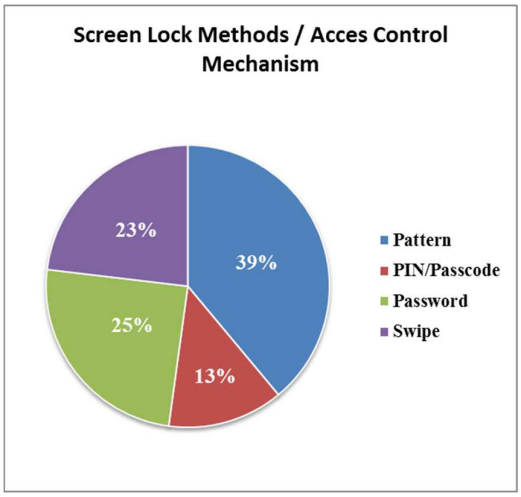


FIGURE 5: SIM CARD LOCK SET UP BY RESPONDENTS

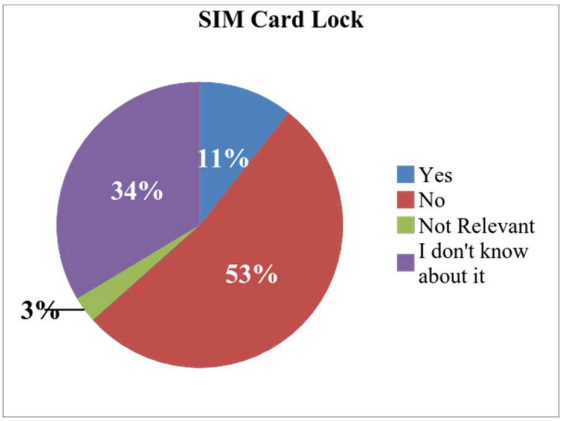


FIGURE 6: INSTALLATION OF ANTIVIRUS ON RESPONDENTS' SMARTPHONE

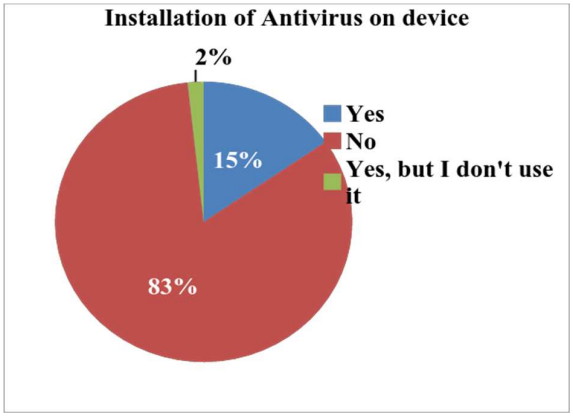


FIGURE 7: INSTALLATION OF APPS FROM UNKNOWN SOURCES

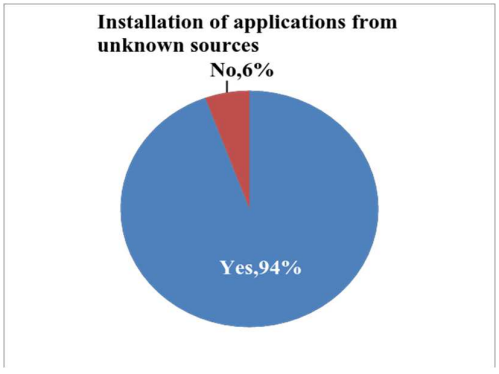


FIGURE 8: RESPONDENTS ATTITUDE TOWARDS APPLICATION PERMISSIONS AND PRIVACY POLICY

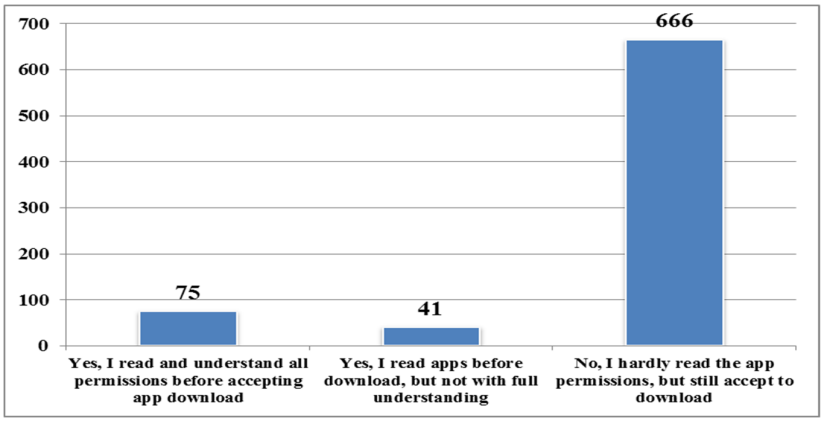


FIGURE 9: INSTALLATION OF ANTI-THEFT OR LOCATING TRACKING APPLICATION

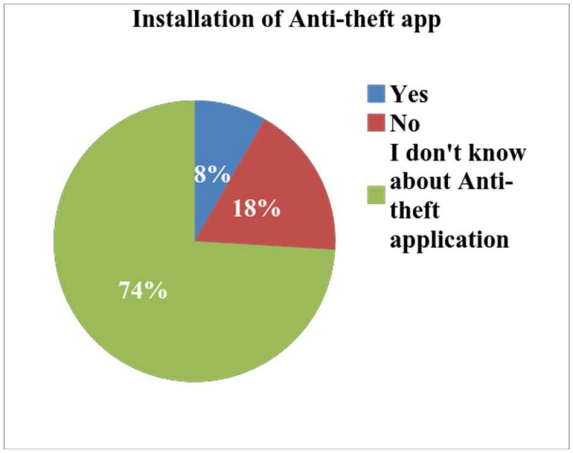
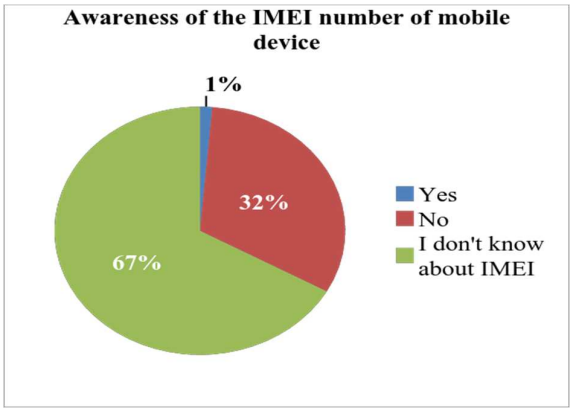


FIGURE 10: IMEI NUMBER WRITTEN DOWN BY RESPONDENTS



V. RESULT & DISCUSSION

The findings of this research were targeted at evaluating the security culture and consciousness of mobile security among smartphones users. The summary of the research is in answering the proposed research questions:

Research Question 1:

What is the level of importance that user's accord to the content or information stored of their smartphone?

Respondents scored that the content or information on their mobile device is of high importance and losing it will be ruinous (Figure 3). This feeling could be a reason for the greater number of respondents recorded for the use of access control mechanism to protect unauthorized entry into the device (Figure 4). Also, respondents had sensitive personal data on their device, alongside the contact list, other information such as ATM and email passwords, Bank Account Numbers, House Numbers, Index Numbers, Passport Numbers, Social Security Numbers, Staff/Employee and Voter IDs.

Research Question 2:

Do smartphone users put in place authentication mechanisms or access control methods to restrict unauthorized access to their device?

It was discovered that most respondents had an access control or authentication mechanism set up, with pattern drawing gaining the prevalence. However, locking of SIM Card was not encouraging (Figure 5). The screen could be locked securely, but the content of the SIM is not protected as just simply removing and inserting into another mobile device will expose all the useful data it contains.

Research Question 3:

Do smartphone users fully read and understand permissions that accompany mobile applications downloaded from the various mobile app stores?

Mobile applications in android has the capacity to read the phone contacts, call logs, content of device's memory, text messages and can determine the approximate or precise location of users of smartphone. Others can directly call phone numbers, send messages, and record audio without the user's intervention and explicit confirmation. But this activity of mobile application is made possible by the user's acceptance of permission during the download and installation of the

applications. Analysis from Figure 8 revealed that majority of the users of smartphones, during the download and installation from the app stores do not thoroughly read and fully understand the permissions but are quick to accept to host the application on their devices. This exposes the low, if not totally slack in security culture and practices on the part of the users.

Research Question 4:

Do smartphone users install security software on their device to detect, protect and offset any security threat?

Figure 6 shows users attitude towards the installation and running of antivirus application as security software to detect and protect their device from malware and any security threat. The figures portray that the use of antivirus among respondents was on the lower side. Particularly when majority of the respondent have toggled on the installation of applications from unknown source (Figure 7), an antivirus would have been a good option to scan for malware and ward off potential harmful applications.

Research Question 5:

Do smartphone users know the availability of anti-theft applications and location tracking services that can be used to trail or remotely wipe their confidential data on their device in case phone lost or theft?

The use of anti-theft applications among respondents of this research also registered low patronage. (Figures 9 and 10) painted the true portrait of respondent's awareness of the usefulness of Siri on iPhones, Android Device Manager, Anti-theft app and IMEI number. The ignorance of respondents stood at 55% did not know about Siri, 60% about Android Device Manager, 74% about anti-theft application and 67% about IMEI. Therefore, in the unfortunate event of misplacing of the smartphone or it being stolen, users are unable track the mobile device.

VI. CONCLUSION

It could be logically concluded that;

- Users treasure the content of their smartphone but lack the security attitude in protecting such delicate information. The deficiency in security awareness reflects respondent's hesitancy to neither install security applications such as antivirus and anti-theft app nor make use of android device manager and siri on their android and iPhone respectively.
- Though respondent's statistics on strong access control method was positively encouraging, there still remains an unsecured hole that is a threat to mobile security. Failing to set up SIM card lock, allowing installation from unknown sources and leaving Bluetooth on and in discoverable (visible) mode still make the device an easy prey to ruthless attackers.
- User's lack of security awareness was also seen in respondent's reluctance to read thoroughly the mobile application permissions and privacy policies that accompany applications.

VII. RECOMMENDATIONS

Based on research findings, the authors would like to recommend the following to smartphone users: -

- Smartphone users should be cautious and wakeful about mobile application permissions and the information the application would want to access before granting permission during installation.
- Smartphones manufacturers, telecommunication service providers as well as the mobile security agencies should enhance security awareness creation to inform users on the various security threats, as well as the security measures and defensive mechanisms needful for maximum protection of the mobile handset and its content against data loss.
- Smartphone users should take advantage of the value of mobile antivirus and anti-theft applications to counter potential mobile malwares and spywares as well locate, protect and restrict access to misplaced or stolen mobile handset.

VIII. SCOPE FOR FURTHER RESEARCH

It is hereby suggested that further studies and a nationwide survey be carried out on this research to ascertain the mobile security attitude of smartphone users as the usage of the device swells exponentially on the national or international level.

REFERENCES

1. Mylonas, A. (2013). *Security and Privacy in the Smartphones Ecosystem.* Athens University of Economics & Business, Informatics. 76 Patission Ave., Athens GR-10434, Greece: Information Security & Critical Infrastructure Protection Research Laboratory.
2. Gartner. (2016). *Gartner IT Glossary*. Retrieved August 24, 2016, from http://www.gartner.com/it-glossary/feature-smartphone/
3. Androulidakis, I., & Kandus, G. (2011). Mobile Phone Security Awareness and Practices of Students in Budapest. *The Sixth International Conference on Digital Telecommunications, ICDT*, p.18.
4. Mitchem, S. C., Dykes, S. G., Cook, S. W., & Whipple, J. G. (2012, March/April). Mobile Applications Security, Safeguarding Data in a Mobile Device Word. *Cross Talk*, p.12.
5. Technavio. (2016, August 24). *Why Mobile Security is More Critical Than You Think*. Retrieved August 28, 2016, from http://www.technavio.com/blog/why-mobile-security-more-critical-you-think
6. Huang, D.-L., Rau, P.-L. P., Salvendy, G., Gao, F., & Zhou, J. (2011, December). Factors affecting Perception of Information Security and their Impacts on IT Adoption and Security Practices. *International Journal of Human-Computer Studies, 69*(12), 870-883.
7. iTexico. (2013, April 16). *Knowing the Mobile App Security Threats & How to Prevent Them*. Retrieved August 26, 2016, from iTexico Blog:http://www.itexico.com/blog/bid/92948/Knowing-the-Mobile-App-Security-Threats-How-to-Prevent-Them
8. Gundu, T., & Flowerday, S. V. (2013). Ignorance to Awareness: Towards an Information Security Awareness Process. *South African Institute of Electrical Engineers* (104), 69-79.
9. MobileIron. (2014). Mobile Security: Threats and Countermeasures. *MobileIron White Paper* (MKT-6361 V1.0), 2-3.
10. Avast. (2015). *Avast, Protecting 230 million people*. Retrieved August 26, 2016, from https://www.avast.com/c-malware
11. Lookout. (2016). Retrieved August 25, 2016, from https://www.lookout.com/know-your-mobile/what-is-a-mobile-threat
12. Microsoft. (2016). *Safety & Security Center*. Retrieved August 25, 2016, from What is Spyware?: https://www.microsoft.com/en-us/saftey/pc-security/spy-ware-whatis.aspx
13. (2012). *Gosafeonline (2012-01)*. Infocomm Development Authority of Singapore.
14. SnoopWall Mobile Security. (2014). *SnoopWall Flashlight Apps Threat Assessment Report: Summarized Privacy and Risk Analysis of Top 10 Android Flashlight Apps.* One Tara Boulevard, Suite 200 Nashua, NH - 03060: SnoopWall Mobile Security Experts and The Privacy App Scanner.
15. Kaspersky Lab. (2016). *Android Mobile Security Threats*. Retrieved August 26, 2016, from https://usa.kaspersky.com/internet-security-center/threats/mo-bile#.V7-GMTNw2mE
16. iTexico. (2013, April 16). *Knowing the Mobile App Security Threats & How to Prevent Them*. Retrieved August 26, 2016, from iTexico Blog:http://www.itexico.com/blog/bid/92948/Knowing-the-Mobile-App-Security-Threats-How-to-Prevent-Them
17. Maslennikov, D. (2011, October). *Zues-in-the-Mobile - Facts and Theories. Kaspersky*. Retrieved August 26, 2016, from http://www.securelist.com/en/analy-sis/204792194/ZeuS_in_the_Mobile_Facts_and_Theories
18. Kulkarni, S. P., & Bojewar, S. (2015, December). Vulnerabilities of Smartphones. *International Research Journal of Engineering and Technology (IRJET), 2*(9), 2422-2426.

19. Niem, T. C. (2003). *Bluetooth And Its Inherent Security Issues.* SANS Institute InfoSec Reading Room.
20. Minar Ibn, N. B.-N., & Tarique, M. (2012, January). Bluetooth Security Threats and Solutions: A Survey. *International Journal of Distributed and Parallel Systems, 3*, 127-148.
21. The Inkerman Group. (2010,June). Smartphone Vulnerabilities: Securing your personal and business data. p. 2.
22. Tu, Z., & Yuan Yufei. (2012). Understanding User's Behaviors in Coping wth Security Threat of Mobile Devices Loss and Theft. *45th Hawaii International Conference on System Sciences* (pp. 1393-1402). IEEE Computer Society.
23. McAfee. (2012). *10 Quick Tips to Mobile Security.* McAfee.
24. Beal, V. (2016). Retrieved September 6, 2016, from http://www.webopedia.com/TERM/C/countermeasure.html
25. IPA. (2012, June 8). Security Measures Guide For Smartphone (Avoidance of Risks). *2nd*, 2-22. Japan: Information-technology Promotion Agency.
26. Consumer Reports. (2014, April). *5 Steps to Protect Your Smart phone form Theft or Loss*. Retrieved September 6, 2016, from http://www.consumerreports.org/cro/2014/04/5-steps-to-protect-your-smart-phone-against-theft-or-loss/index.htm
27. Dawson, T. (2015, June 16). *Android Headlines*. Retrieved September 8, 2016, from http://www.androidheadlines.com/2015/06/featured-top-10-anti-theft-android-apps.html
28. Knoll, M. (2014, January 25). *How To Keep Your Android Phone From Getting Lost And Stolen*. Retrieved September 8, 2016, from http://trendblog.net/how-to-protect-your-android-device-from-being-lost-stolen/
29. Consumer Reports. (2014, April). *5 Steps to Protect Your Smart phone form Theft or Loss*. Retrieved September 6, 2016, from http://www.consumerreports.org/cro/2014/04/5-steps-to-protect-your-smart-phone-against-theft-or-loss/index.htm
30. *HackTrix*. (2016). Retrieved September 8, 2016, from How To Track and Block Lost or Stolen Mobile Phone Using its IMEI Number: http://www.hacktrix.com/track-block-lost-stolen-mobile-phone-using-imei-number
31. Luo, S., & Yan, P. (2014). Fake Apps Feigning Legitimacy. *A Trend Micro Research Paper*. Texas 75062, U.S.A: Trend Micro Incorporated.
32. Perez, S. (2016, July 18). *Beware the Fake Pokemon Go apps*. Retrieved September 12, 2016, from TechCrunch:https://techcrunch.com/2016/07/18/beware-the-fake-pokemon-go-apps/
33. Neal, R. W. (2014, July 4). *Google Removes Top App: 'Virus Shield' Scams Thousands, Exposes Flaw in Android Ecosystem.* Retrieved September 12, 2016, from International Business Times: http://www.ibtimes.com/google-removes-top-app-virus-shield-scams-thousands-exposes-flaw-android-ecosystem-1568362
34. Zhang, V. (2014, February 11). *Trojanized Flappy Bird Goes on the Heels of Takdedown by App Creator*. Retrieved September 12, 2016, from TrendLabs Security Intelligence Blog: http://www.blog.trendmicro.com/trendlabs-security-intelligence/trojanized-flappy-bird-comes-on-the-heels-of-takedown-by-app-creater/
35. Kovacs, N. (2016, February 23). *The Risks of Third Party App Stores*. Retrieved September 12, 2016, from Norton Protection Blog: https://community.norton.com/en/blogs/norton-protection-blog/risks-third-party-app-stores
36. Liccardi, I., Pato, J., & Weitzner, D. J. (2013). Improving Mobile App Selection through Transparency and Better Permission Analysis. *Journal of Privacy and Confidentiality* (5, Number 2), 5-7.
37. Sanchez, M. (2012, June 12). *Are You Aware of the Dangers Lurking in Free Apps?* Retrieved September 14, 2016, from Cisco Blogs: http://blogs.cisco.com/smallbusiness/are-you-aware-of-the-dangers-lurking-in-free-apps
38. MetaFilter. (2010, August 26). *User-driven Discontent*. Retrieved September 14, 2016, from MetaFilter Community Weblog: http://www.metafilter.com/95152/Userdrive-discontent#3256046
39. Ghana Statistical Service. (2014). *2010 Population & Housing Census District Analytical Report, Tarkwa Nsuaem Municipality.*
40. Creative Research Systems. (2012). *The Survey System*. Retrieved September 2, 2016, from Sample Size Calculator: http://www.surveysystem.com/sscalc.htm

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application & Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you to supply your critical comments and suggestions about the material published in this issue, as well as on the journal as a whole, on our e-mail **infoijrcm@gmail.com** for further improvements in the interest of research.

If you have any queries, please feel free to contact us on our e-mail **infoijrcm@gmail.com**.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward to an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-
Co-ordinator

DISCLAIMER

The information and opinions presented in the Journal reflect the views of the authors and not of the Journal or its Editorial Board or the Publishers/Editors. Publication does not constitute endorsement by the journal. Neither the Journal nor its publishers/Editors/Editorial Board nor anyone else involved in creating, producing or delivering the journal or the materials contained therein, assumes any liability or responsibility for the accuracy, completeness, or usefulness of any information provided in the journal, nor shall they be liable for any direct, indirect, incidental, special, consequential or punitive damages arising out of the use of information/material contained in the journal. The journal, neither its publishers/Editors/ Editorial Board, nor any other party involved in the preparation of material contained in the journal represents or warrants that the information contained herein is in every respect accurate or complete, and they are not responsible for any errors or omissions or for the results obtained from the use of such material. Readers are encouraged to confirm the information contained herein with other sources. The responsibility of the contents and the opinions expressed in this journal are exclusively of the author (s) concerned.

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals