International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 08 | Aug 2018 www.irjet.net p-ISSN: 2395-0072

Awareness and knowledge about Android smartphones security among Ghanaians

Kwame Ofosuhene Peasah, Michael Asante

Department of Computer Science, Kwame Nkrumah University of Science and Technology, Ghana

---

Abstract: The intent of deletion, factory resetting as well as flashing of user's mobile device is to conceal sensitive data or information from a third party or anonymous user. However, if the application of these commonly used data wiping methodologies fails to achieve their intent, then the user may appear to be "naked" or vulnerable (susceptible to possible electronic related crime attack). Considering the Android OS design flaws in data erasure, and subsequent abundance and dominance of Android smartphones in recent years, the study assessed users' awareness and knowledge about Android smartphones security in Ghana. Adopting the cross-sectional design and simple random sampling technique, 1240 respondents aged 18 years and above were sampled for the study. Result indicates that majority of the study participants had previously owned an Android smartphone and were either keeping it or gave it out. Photos, videos, audios, office documents, notes and contacts were considered private data yet email, financial transactions, and health, academic and social information were information frequently accessed. Using the binary logit model, respondents' gender and age predicted their knowledge and awareness, respectively, on data encryption and data recovery. The vulnerability level of respondents to malicious attacks was rated as high and as such, the study recommends the need for awareness campaign among Smartphone users so as to reduce their tendencies to cybercrime and malicious attacks in the event of theft, misplaced and/or damaged phone.

1. INTRODUCTION

The penetrative ability of several smartphones may be largely attributed to the popularity and availability of the android operating system. The popularity of the Android OS market dominance is buttressed by the International Data Corporation (IDC) statistical report in which the market share of Android smartphone market was 85% in 2017 (IDC, 2017). Its popularity though advantageous, makes it a lucrative avenue for attacks by malicious attackers. Designed as an open, programmable network device with the capacity to operate as PCs, smartphones plays an increasingly important role in personal life and also carries massive classified and private data due to its massive non-volatile memory (Wilcox, n.d.).

Basically, smartphone is a cell phone with Internet access and built-in applications such as email, web browsing, audio, and video players (PC Magazine, n.d.). Smartphones are effective in accessing personal and corporate email, prepare tax returns, and review customer documents and web browsing, besides its primary function of communication, calling (Dagon et al. 2004; Yu et al. 2014; McAfee Inc. n.d.). Nathan and Xiandong (2017) not only acknowledged the prevalence of smartphones notably those with Android Operating System (AndroidCentral, 2016) but also recognised the surge of applications available on such devices which process a significant amount of personal information. Unfortunately, given the popularity of smartphones, coupled with its intrinsic mobility and the rise of the threats to smartphone data, the device is vulnerable to attacks once it is lost, stolen, misused or damaged thus losing sensitive information such as contacts, messages, photos, credit card information and passwords. Such vulnerability compromises the confidentiality, integrity, and availability of data and services once the phone fall into the hands of malicious people (Dagon et al. 2004; Yu et al. 2014; Muslukhov, 2012).

Amidst the vulnerabilities associated with the use of smartphones, the device act as effective mediums for disseminating video-based healthcare intervention (Jones and Lacroix, 2012). For instance, cell phones have been effective in a range of telehealth applications (Ackerman et al. 2010; Doam et al. 2009), health promotion (Lester et al. 2010; Mitchell et al. 2011; Puccip et al, 2006; Swendeman et al. 2010) reducing HIV risk through short videos (Cornelius et al. 2011) and promoted smoking cessation (Whittaker et al. 2011; Whittaker et al. 2008).

Globally, market for smartphones keeps increasing and will outgrow that of personal computers, notebooks and netbooks internationally (Stanley, 2009) due to the convenience and availability of diverse application especially on Android phones (Seo et al. 2012). Markets for Android and iOS smartphones stands at 99.7% (IDC, 2017a), having climbed above 90% in the first quarter of 2014 (International Data Corporation [IDC], 2014) and 80% in 2013 (Zhou et al. 2014). Moreover, the IDC in 2014 predicted that out of the 1.2 billion new smartphones which will be shipped, nearly 79% (over 950 million) would be powered by Android OS (IDC, 2014). Whereas sale of smartphone was in excess of 45% in the developed world in 2011 (Gartner Group, 2011; Smith, 2010, 2011), that of developing world, especially Ghana, was at 51% (Mobile Africa, 2015). These significant increases arguably, makes Android one of the greatest success stories of the software industry of the last few years (Armando et al. 2012).

In spite of this, the open source application provided by Android makes its system vulnerable, and susceptible to malicious attacks such as viruses, Trojan horses and worms (Cho and Moon, 2011; Shabtai et al. 2010; Zakorzhevsky , 2011; Eric, 2011). This vulnerability stems from the Android OS design flaws in data erasure which makes it very easy to recover deleted data from an Android device even after a factory reset has been performed (Shu et al. 2017). The effect of these attacks are synergistic in nature as the user and the cellular service provider tend to experience the effect alike. For instance, the introduction of a malware could disable a smartphone, especially Android, partially or fully and cause unwanted billing, steal private information (possibly by phishing and social engineering methods); or infect every name in a user's phonebook (Piercy, 2004; Dikinson, 2005; Muthukuma et al., 2008).

The problem of data protection in smartphones is an important and challenging task given the threat of mobile phones to being lost, stolen, or infested with virus infection (Muslukhov et al. 2012). Although Android smartphones are plagued with data deleting flaws, users of Android smartphones almost always make use of the default deletion and/or factory reset functions thus, making data recovery on second hand phones easily accessible. This study assessed smartphone users' awareness and knowledge about Android security among the Ghanaian population by examining the medium used by smartphone users' in disposing of their used phones, the amount of relevant and critical data that resides on a smartphone after its contents have been hidden, deleted or wiped, parameters for securing information on Android smartphones and options available to users' after disposing of their used phones.

2. METHODS

2.1 Study design and context

A population-based, cross-sectional quantitative study was conducted to assess the community's knowledge and vulnerability awareness in the use of smartphone with Android OS in Ghana. The quantitative design ensured the independence of the researcher from the study findings and is also premised on the assumption that there is a social reality external to the knower and knowledge is objective and tangible (Patton, 2002; Long, 2014). The study also drew on the empiricist paradigm (Creswell, 2003) in which the investigator is capable of studying a phenomenon without influencing it or being influenced by it; "inquiry takes place as through a one way mirror" (Guba and Lincoln, 1994: 110). Thus, great emphasis is placed on ensuring validity of the research findings by the process of rigorous clarification and reliability through the use of statistical tests (Milne n.d). In view of this, large sample sizes are used so as to ensure representativeness of the study findings (Carey, 1993). The study instrument was divided into two sections. Section 'A' elicited data on the biodata of respondents: gender, age, educational level and current phone model used. Some of data sought from section 'B' include information usually accessed/stored on your phone, mode of disposing used phone, information considered to be private, mode of getting rid of private data before disposing of phone, knowledge about encryption of Android phones and means used to retrieve deleted files.

The study transcends the administrative boundaries of Ghana located at the centre of the West African sub-region. With a total land size of 238,533 square kilometres, Ghana lies between Latitudes 4^{o} and 12^{o} North and Longitudes 4^{o}W and 2^{o} East. The country shares boundaries with three Francophonic countries: Cote D'ivoire to the west, Togo to the east, and Burkina Faso to the north, with the Gulf of Guinea and the Atlantic Ocean to the south (Ghana Statistical Service [GSS], 2016). About 48 percent of Ghana's population own mobile phones while only 7.8 percent use internet facility (Ghana Statistical Service [GSS], 2014).

2.2 Sample and Procedure

Individuals aged 18 years and above were included in the study since this age is defined as the maturity age in Ghana where one is eligible to make informed decisions (GSS, 2016). A sample study of 1240 was randomly selected for the study and was representative of the total population in the country. Respondents for the study were sampled from various households across the length and breadth of the country from October, 2016 to December, 2016. However, in order to ensure the reliability of the research instrument, the questionnaires and participatory activities were pre-tested by the researcher and his team (Research and Teaching Assistants) in the Kwame Nkrumah University of Science and Technology (KNUST): a pilot study was embarked upon and questions which were not clear were clarified before launching out for the main study. The final instrument sought information on respondents' biodata, previous phone used and mode of disposal, predominant activities undertaken on the phone and knowledge about Android security and data recovery techniques. Each interaction with the respondents lasted averagely for 25 minutes.

2.3 Data management and analysis

The edited data was captured in the Predictive Analytics SoftWare (PASW) version 16 and analysed using descriptive and inferential statistics. The descriptive statistics were presented by means of tables whereas some were converted into bar graphs using Microsoft excel 2013. Since respondents used different models of smartphones (Android and non-Android),

the data was split using the "split data" and "select cases" command in the PASW so that cases of respondents who use Android smartphones could be analysed. The options for mode of phone disposal was further recoded from its initial five options (sold, gift, exchange, stolen/missing and still keeping) to two variables: sold, gift, stolen/missing and exchange were recoded as 'gave it out' whereas still keeping was maintained. Besides this, chi-square test analysis was used to examine relationship between the study variables. Also, binary logit model was used to predict respondents' knowledge on Android security and data recovery based on their biodata. The outcome variable was: "Do you know of encryption of Android phones?" and were optioned as "Yes/No". Both the chi-square test and regression analysis were significant at $p<0.05$.

2.4 Ethical consideration

The purpose of the study was explained to all the respondents and were assured of the confidentiality and privacy of the information they provide. Participants were informed that the study is purely for academic purposes and that, participation was voluntary. Besides this, all the research team presented their identification cards as proof of their affiliation to the Department of Computer Science, Kwame Nkrumah University of Science and Technology (KNUST).

3. RESULT

3.1 Biodata of Respondents

From the study result, majority were males (760, 61%), within the 18-24 age cohort (918, 74%), were first degree holders (970, 78%) and were using Android powered smartphones (1040, 84%) as illustrated in Table 1.

Table 1: Demographic Characteristics of Respondents

Variable	Frequency (N=1240)	Percent (%)
Gender		
Male	760	61.3
Female	480	38.7
Age		
18-24 years	918	74
24-30 years	58	4.7
31 years or more	264	21.3
Educational level		
No education	9	.7
Basic education	27	2.2
SHS/Technical/Vocational	234	18.9
Tertiary	970	78.2
Phone in use		
Android phone	1040	83.9
Windows phone	28	2.3
Apple	114	9.2
Non-smart phone (yam)	58	4.7

3.2 Previous phone used and mode of disposal

The study discovered that almost all respondents across the various demographic category previously owned an Android smartphone. Overall, males (706, 62%) aged 18-24 years (820, 72%) and were first degree holders (880, 77%) had previously used Android phones. However, across all the various demographic spectrum, Samsung smartphones were the main Android phone model used by the respondents. All the responses were significant at $p<0.05$ (Table 2).

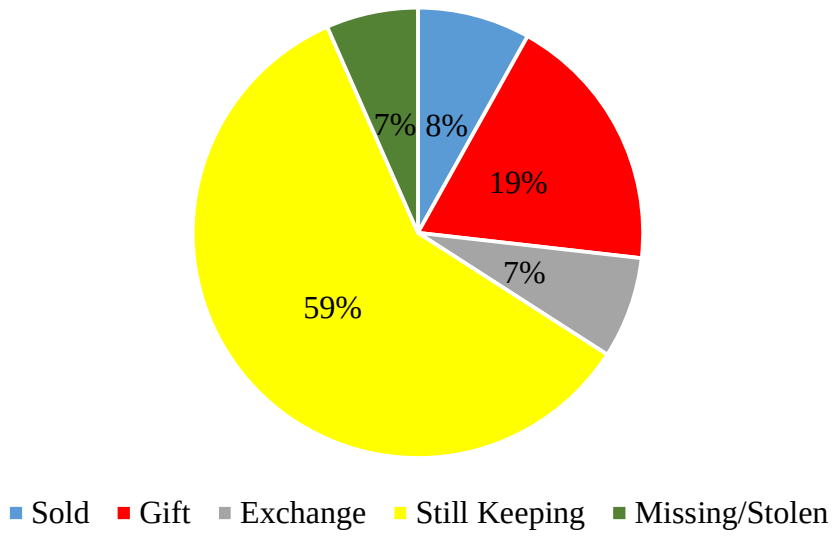
Table 2: Chi-square test of previous phone used by biodata of respondents

Variables	Type of phone model used							*p-value*
	Samsung	Huawei	LG	Infinix or itel	Tecno	Other Android phones	Total	
Gender								
Male	358 (62.7)	34 (43)	38 (66.7)	106 (54.4)	91 (69.5)	79 (73.1)	706 (61.9)	0.000*
Female	213 (37.3)	45 (57)	19 (33.3)	89 (45.6)	40 (30.5)	29 (26.8)	435 (38.1)	
Age								
18-24 years	369 (64.6)	49 (62)	47 (82.5)	152 (77.9)	96 (73.3)	107 (99.1)	820 (71.9)	0.000*
24-30 years	41 (7.2)	3 (3.8)	1 (1.7)	7 (3.6)	4 (3.0)	1 (0.9)	57 (5)	
31 years or more	161 (28.2)	27 (34.2)	9 (15.8)	36 (18.5)	31 (23.7)	0 (0)	264 (23.1)	
Educational level								
No education	4 (0.7)	0 (0)	3 (5.3)	0 (0)	2 (1.5)	0 (0)	9 (0.8)	0.000*
Basic education	12 (2.1)	1	0 (0)	8 (4.1)	6 (4.6)	0 (0)	27 (2.4)	
SHS/Technical/ Vocational	107 (18.7)	24	3 (5.3)	33 (16.9)	34 (25.9)	24 (22.2)	225 (19.7)	
Tertiary	448 (78.5)	54	51 (89.5)	154 (79)	89 (67.9)	84 (77.8)	880 (77.1)	

*The Chi-square statistic is significant at the 0.05 level.

Besides the above responses, the study sought information on the mode of disposal of the previous phone depending on whether respondents ever did that. With this, majority were still keeping their previous phones (59%) whereas the remaining had either given it out as a gift, exchanged it, sold it or had the phone stolen (Figure 1).

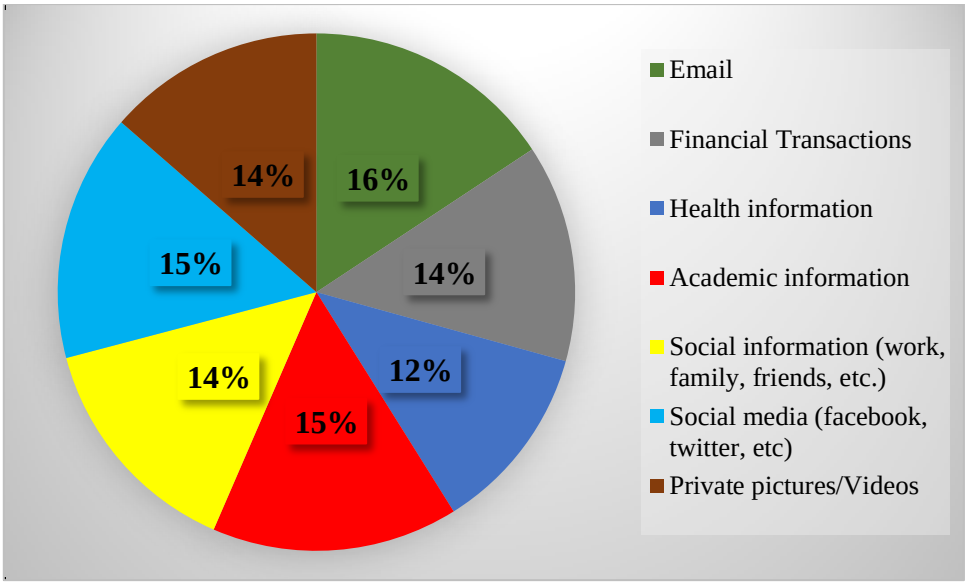
Figure 1: Mode of disposal of previous phone



3.3 Android phone users, information accessed and data privacy

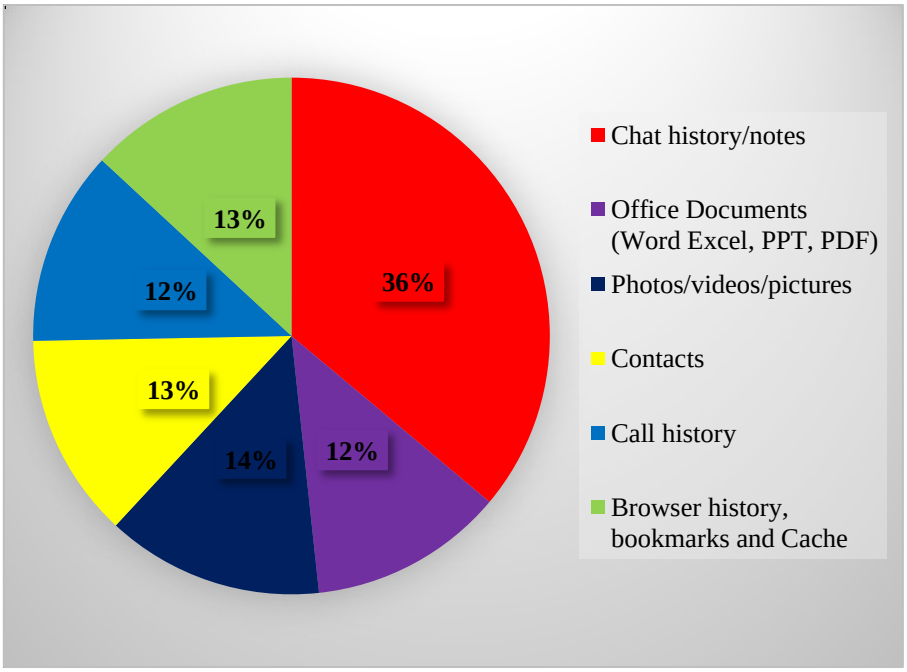
The study found that 1040 of the study participants used Android smartphones. As regards the type of information frequently accessed on it, these ranged from accessing email, financial transactions, and health, academic and social information (Figure 2).

Figure 2: Information frequently accessed on phone



In spite of this, the type of data considered private or sensitive by respondents include chat history/notes, photos/videos/pictures, office document, contacts and videos (Figure 3).

Figure 3: Type of data considered private



A chi-square test analysis between medium of phone disposal and awareness about accessing deleted files and means to getting rid of private data before disposing of phone shows that majority (965, 77.8%, *p=0.094*) who either gave out or still kept their phone were aware that data from an Android phone can be accessed after it has been deleted or the device has been reset. This notwithstanding, with regards to the means to getting rid of private data before disposal, whereas majority (500, 40%) of the smartphone users did nothing as regards formatting the memory card (sdcard) (*p=0.024*), some 31% (certain/very certain, 31.5) definitely formatted the memory card. Likewise, whereas 37% did nothing in reference to performing a factory reset (*p=0.048*), some 35% (certain/very certain, 35.3%) undertook this process as illustrated in Table 3.

Table 3: Chi-square test on medium of phone disposal and private data protection

		Medium of disposing of phone			*p-value*
		Gave it out	Still keeping	Total	
		N=496 (%)	N=744 (%)	N=1240 (%)	
Awareness about accessing data after deletion or reset	Yes	374 (75.4)	591 (79.4)	965 (77.8)	0.094
	No	122 (24.6)	153 (20.6)	275 (22.2)	
Delete specific items from the device	Least likely	61 (12.3)	69 (9.3)	130 (10.5)	0.224
	Likely	74 (14.9)	95 (12.8)	169 (13.6)	
	Do Nothing	142 (28.6)	212 (28.5)	354 (28.5)	
	Certain	73 (14.7)	131 (17.6)	204 (16.4)	
	Very certain	146 (29.4)	237 (31.8)	383 (30.9)	
Format the memory card (sdcard)	Least likely	77 (15.5)	118 (15.9)	195 (15.7)	0.024*
	Likely	79 (15.9)	75 (10.1)	154 (12.4)	
	Do Nothing	185 (37.3)	315 (42.3)	500 (40.3)	
	Certain	46 (9.3)	82 (11)	128 (10.3)	
	Very certain	109 (22)	154 (20.7)	263 (21.2)	
Perform a factory reset on the phone	Least likely	87 (17.5)	141 (18.9)	228 (18.4)	0.048*
	Likely	57 (11.5)	58 (7.8)	115 (9.3)	
	Do Nothing	171 (34.5)	288 (38.8)	459 (37)	
	Certain	47 (9.5)	87 (11.7)	134 (10.8)	
	Very certain	134 (27)	170 (22.8)	304 (24.5)	
Use a "secure deletion" app to erase the phone memory/memory card	Least likely	147 (29.6)	205 (27.5)	352 (28.4)	0.446
	Likely	65 (13.1)	89 (12)	154 (12.4)	
	Do Nothing	220 (44.3)	362 (48.7)	582 (46.9)	
	Certain	34 (6.8)	38 (5.1)	72 (5.8)	
	Very certain	30 (6)	50 (6.7)	80 (6.4)	
Encrypt the phone, then reset	Least likely	145 (29.2)	202 (27.1)	347 (28)	0.164
	Likely	57 (11.5)	61 (8.2)	118 (9.5)	
	Do Nothing	215 (43.3)	367 (49.3)	582 (46.9)	
	Certain	26 (5.2)	42 (5.6)	68 (5.5)	
	Very certain	53 (10.7)	72 (9.7)	125 (10.1)	

*The Chi-square statistic is significant at the 0.05 level.

3.4 Knowledge and awareness about Android security and data recovery

Considering the type of information accessed on these phones, as well as those cogitated as private, the participants' knowledge about the encryption of Android phones were asked using respondents biodata as predictors. The binary logit

model shows that females had a higher odd of knowing about encryption of Android phones [OR=1.609, 95% CI (1.274 - 2.031)] as compared to their male counterparts. The remaining demographic characteristics had some predictive effect but were all insignificant (Table 3).

Table 3: Predictors of knowledge about encryption of Android phones

Covariates	Do you know of encryption of Android phones? Yes/No		
		OR	95% CI
Gender	Male	1	
	Female	1.609	1.274 - 2.031*
Education	No education	1	
	Basic education	1.101	0.233 - 5.203
	SHS/Technical/Vocational	1.166	0.298 - 4.568
	Tertiary	0.883	0.229 - 3.404
Current phone used	Android phone	1	
	Windows phone	0.702	0.326 - 1.509
	Apple	1.268	0.856 - 1.879
	Non-smart phone (yam)	1.517	0.854 - 2.696

*Statistically significant at $p<0.05$.

Although majority (78%) of the study participants were knowledgeable about the fact that data from an Android phone can be accessed after it has been deleted or the device has been reset, this had no relation with the demographic characteristics besides their age. The binary logit model in Table 4 shows that respondents who were 31 years and above [OR=0.381, 95% CI (0.248-0.585)] had a lesser odd of being aware about Android data recovery in comparison to those between 18 and 24 years.

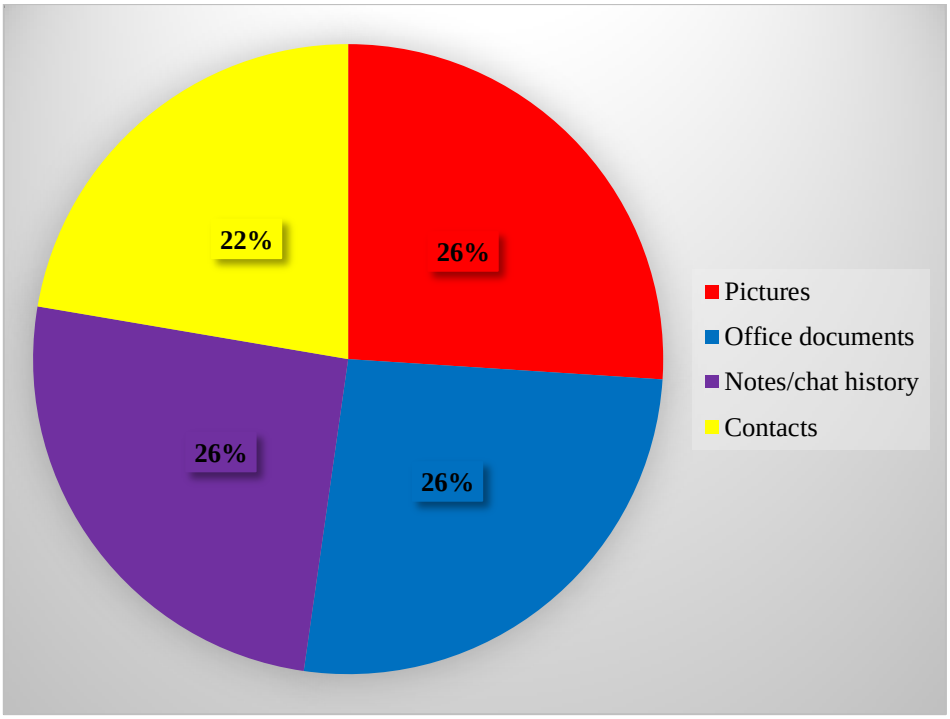
Logistic regression model on awareness about Android data recovery

Covariates	Awareness about Android data recovery? Yes/No		
		OR	95% CI
Age	18-24 years	1	
	24-30 years	0.565	0.275-1.160
	31 years and above	0.381	0.248-0.585*
Gender	Male	1	
	Female	1.145	0.867-1.513
Education	No education	1	
	Basic education	0.663	0.127-3.453
	SHS/Technical/Vocational	0.258	0.060-1.117
	Tertiary	0.305	0.072-1.300
Current phone used	Android phone	1	
	Windows phone	0.302	0.070-1.295
	Apple	1.124	0.716-1.765
	Non-smart phone (yam)	0.877	0.411-1.869

*Statistically significant at $p<0.05$.

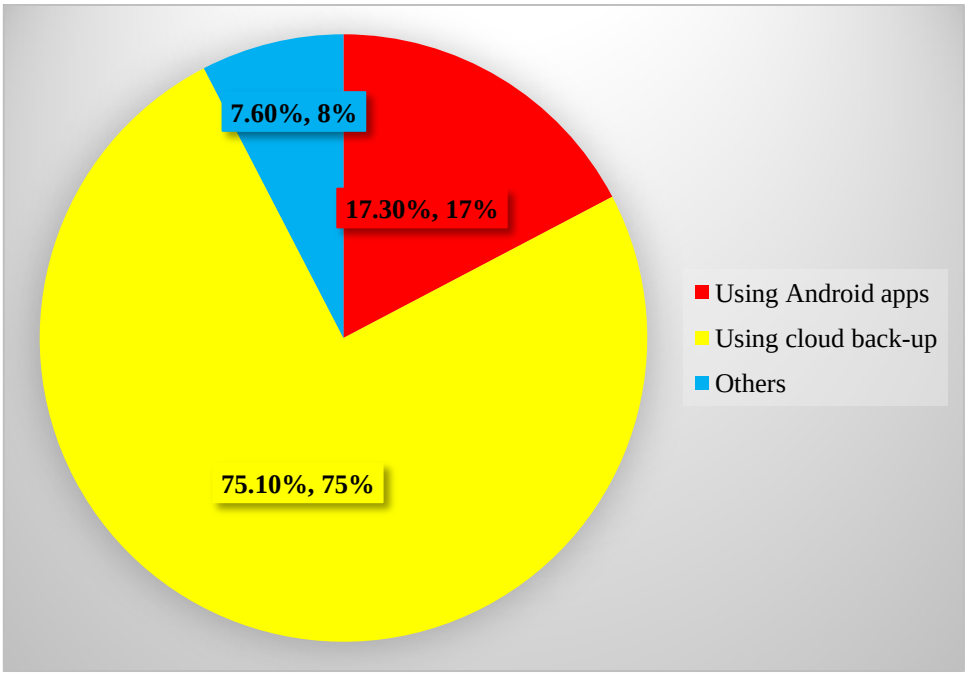
Among those who had ever accessed any of their deleted files, the contacts, notes, office documents and pictures were the main files which were retrieved (Figure 4).

Figure 4: Types of files accessed



The study further found that Android apps (17%) and cloud back-up (75%) were the main tools used by respondents to retrieve deleted files on their phones in the event of deletion and/or factory reset as depicted in Figure 5.

Figure 5: Means used to retrieve deleted files



3.5 Parameters for securing information on Android phones

In view of the study objective, the data was split by selecting cases of Android smartphone use only among the respondents. Using measures of central tendencies (Mean and standard deviation), the study discovered that whereas an average of 0.2, with a deviation of 0.4 had google account saved on their phone, only an average of 0.04 and a deviation of 0.2 had it synchronised with their phone. Likewise, an average of 0.3 with a deviation of 0.4 had a password or lock pattern on their phone (Table 5).

Table 5: Parameters for reducing vulnerability of Android smartphones

Parameter	Mean	Standard Deviation
Do you have a google account (gmail account)	0.1606	0.36732
If yes, do you log into your account on your phone (synchronise)	0.0378	0.19082
Was there a password or lock pattern on your phone whiles in use	0.2779	0.44817
a. What type of phone do you use currently? = Android phone		

4. DISCUSSION

The current study have assessed the level of vulnerability of Android smartphone users by ascertaining their knowledge and awareness about Android smartphones security in Ghana. Based on the study findings, the predominant activities undertaken on the smartphone include, but not limited to accessing email, financial transactions, and health, academic and social information. This proves that smartphones are effective in accessing personal and corporate email, prepare tax returns, and review customer documents and web browsing, besides its primary function of communication, calling (Dagon et al. 2004; Yu et al. 2014; McAfee Inc. n.d; Meshram and Thool, 2014). Although the frequent activities undertaken on the phone included financial transactions and electronic mails, the study participants' viewed their photos, videos, audios, office documents, notes and contacts as private information which needs to be protected from the eye of the public. Perhaps, given the upsurge increase in the leak of private and sensitive photos and videos from the smartphones of individuals with tendencies of destroying their reputation, users tend to place premium on these information. For instance, criminal justice agencies throughout the world are being confronted with an increased need to investigate crimes perpetrated partially or entirely over the internet or other electronic media. Resources and procedures are needed to effectively search for, locate, and preserve all types of electronic evidence. Such evidence according to Lee et al. (2001) range from images of child pornography to encrypted data used to further a variety of criminal activities.

Ironically, though password or lock pattern helps to prevent unauthorised access to one's phone, just a handful of the respondents had their phones protected with either of the two. This behaviour as identified among the study participants is rather unfortunate, given the popularity of Android smartphones, its intrinsic mobility and susceptibility of smartphone data to malicious attacks (Cho and Moon, 2011; Shabtai et al. 2010; Zakorzhevsky, 2011; Eric, 2011). This practice rather increases the vulnerability of the device attacks once it is lost, stolen, misused or damaged thus losing sensitive information such as contacts, messages, photos and videos (Ghana News Agency, 2009). In the Miami phone theft incidence, 54% of the theft victims had no locks, such as passwords or PIN-codes, on their phones hence, increasing the vulnerability of sensitive information to second and third parties (Lost and Found, n.d.). In our study, considering the fact that a little of over half of the respondents (59%) were still keeping their previous Android phones and majority do nothing to retrieve sensitive information in the event of a disposal, such vulnerability compromises the confidentiality, integrity, and availability of data and services once the phone fall into the hands of malicious people (Dagon et al. 2004; Yu et al. 2014; Muslukhov, 2012). This indicates that personal information stored on smartphones is prone to leakage (Meshram and Thool, 2014).

That notwithstanding, respondents were knowledgeable and aware of the fact that information saved on their smartphones could be retrieved once deleted or in the event of a factory reset. Not only were respondents in the know of it but have ever used it. Contacts, notes, office documents and pictures were the main files ever retrieved by the respondents. In spite of this, the study findings suggests that most of the respondents are not in the know that google backs most of these information for future retrieval once they synchronise their gmail account on their Smartphones. This is inferred from the abysmal average of 0.04 having synchronised their google account though a significant portion of the respondents had google account. Perhaps, majority of these respondents might not have heard about the on-going universal awareness on the need to secure privacy information or data on Smartphones (Seung-Hyun et al. 2012).

Considering the greater level of security obtained through encryption of smartphones: only persons with the right password can access encrypted data in the event the phone is lost or stolen (Pewter, 2016). The study further reports that respondents' gender significantly predicted their knowledge on encryption of Android phones and age was a predictor of awareness about Android data security. That notwithstanding, most respondents often do not encrypt their phones though it offers better security in comparison to the usual deletion and factory reset. The limitation to this study is that, it did not seek information on security mechanisms such as antimalware and antispam software, host-based intrusion detection tools, and firewalls which are capable of securing information on mobile phones exist among the study participants (Shabtai et al. 2010).

5. CONCLUSION

The study generally reports that respondents have a fair knowledge, and were aware about Android phone security. However, this was dependent on their gender and age respectively. Respondents' knowledge centred mainly on data recovery through the use of cloud back-up in the event of deleting sensitive information. Though respondents' knowledge about Android phone encryption was dependent on their gender, they barely used it. Amidst all these, the vulnerability level of respondents to malicious attacks could be rated as high considering the fact that most of the Smartphones were not password protected and participants rarely made any attempt to retrieve information from their phones before disposing it off. Given the sensitivity of Android Smartphones to malicious attacks (Cho and Moon, 2011; Piercy, 2004; Dikinson, 2005), the data deletion flaws of Android Smartphones and the increasing infiltration of Android Smartphones into the market of both developed (Gartner Group, 2011; Smith, 2010, 2011) and low- and middle- income countries, especially, Ghana (Mobile Africa, 2015), the study recommends the need for awareness campaign among Smartphone users so as to reduce their tendencies to cybercrime and malicious attacks in the event of theft, misplaced and/or damaged phone. Also, the study recommends an improvement in the Android operating system with regards to data deletion.

REFERENCE

- Shu, J. Zhang, Y., Li, J., Li, B. and Gu, D (2017). Why Data Deletion Fails@ A Study on Deletion Flaws and Data Remanence in Android Systems. ACM Trans. Embed. Comput. Syst. 16, 2. DOI: http://dx.doi.org/10.1145/3007211
- Pewter R. (2016). The Pros And Cons Of Android Encryption. Accessed at https://maxwell.en.softonic.com/blog/security-warrior/the-pros-and-cons-of-android-encryption on 1/5/2018.
- Ghana Statistical Service [GSS], (2016). 2010 population and housing census. Summary report of final results.
- International Data Corporation [IDC] (2017a). Smartphone OS Market Share, 2017 Q1. Accessed at https://www.idc.com/promo/smartphone-market-share/os on January 15, 2018.
- Botha, R.A., Furnell, S.M., Clarke, N.L., 2009. From desktop to mobile: examining the security experience. Computer and Security 28, 130–137.
- Muslukhov, I, Boshmaf, Y., Kuo, C., Lester, J., and Beznosov, K (2012). Understanding Users' Requirements for Data Protection in Smartphones. IEEE 28th International Conference on Data Engineering Workshops.
- Piercy, M., 2004. Embedded devices next on the virus target list. IEE Electronics Systems and Software 2, December–January, pp. 42–43.
- Muthukumaran, D. et al., 2008. Measuring integrity on mobile phone systems. In: Proceedings of the 13th ACM Symposium on Access Control Models and Technologies.
- Dikinson, J., 2005. The new antivirus formula. http://www.ironport.com/pdf/ironport_new_anti-virus_formula.pdf.
- Shabtai, A., Fledel, Y., and Elovici, Y. *(2010).* Securing Android-Powered Mobile Devices Using SELinux. COPUBLISHED BY THE IEEE COMPUTER AND RELIABILITY SOCIETIES. 1540-7993/10/$26.00
- Taenam Cho and Nammee Moon, "Smartphone Application Development and Code-signing," KIISC, vol.21 no.1, pp.19-25, 2011
- Armando, A., Merlo, A., Migliardi, M., and Verderame, L. (2012). Would You Mind Forking This Process? A Denial of Service Attack on Android (and Some Countermeasures). Dimitris Gritzalis; Steven Furnell; Marianthi Theoharidou. 27th Information Security and Privacy Conference (SEC), Heraklion, Crete, Greece. Springer, IFIP Advances in Information and Communication Technology, AICT-376, pp.13-24, 2012, Information Security and Privacy Research.
- Gartner Group. (2011). *Press Release*, November 2011. Accessed at http://www.gartner.com/it/page.jsp?id=1848514 on November 9, 2017.
- Smith A. Pew Internet [Internet]. Mobile access 2010. Washington, DC: Pew Research Center; 2010.

- Smith A. Pew Internet [Internet]. Smartphone adoption and usage. Washington, DC: Pew Research Center; 2011.
- Zhou, X., Lee, Y., Zhang, N., Naveed, M., and Wang, X. (2014). The Peril of Fragmentation: Security Hazards in Android Device Driver Customizations. IEEE Symposium on Security and Privacy. DOI 10.1109/SP.2014.33
- Ghana News Agency [GNA] (2009). Police: Crime rate in Greater Accra declines in Accra. Accessed at https://www.ghanabusinessnews.com/2009/01/13/police-crime-rate-in-greater-accra-declines-in-accra/ on November 9, 2017.
- Morgan Stanley [Internet]. The mobile internet report. New York: Morgan Stanley Research; 2009.
- International Data Corporation [IDC] Worldwide Mobile Phone Tracker, Accessed at http://www.idckorea.com/ on November 9, 2017.
- Seo, S-H., Lee, D.G., Yim, K. "Analysis on Maliciousness for mobile application", IMIS 2012, pp. 126-129, 2012.7
- Whittaker R, Dorey E, Bramley D, Bullen C, Denny S, Elley CR, et al. A theory-based video messaging mobile phone intervention for smoking cessation: randomized controlled trial. J Med Internet Res. 2011;13(1):e10.
- Whittaker R, Maddison R, McRobbie H, Bullen C, Denny S, Dorey E, et al. A multimedia mobile phone-based youth smoking cessation intervention: findings from content development and piloting studies. J Med Internet Res. 2008;10(5):e49.
- "Lost and found: The challenges of finding your lost or stolen phone, "http://blog.mylookout.com/2011/07/lost-and-found-the-challenges-offinding-your-lost-or-stolen-phone/.
- V. Zakorzhevsky, "Monthly malware statistics, march 2011,"http://www.securelist.com/en/analysis/204792170/Monthly Malware Statistics March 2011, last accessed November 9, 2017.
- C. Eric, "The motivations of recent android malware. "http://www.symantec.com/content/en/us/enterprise/media/security response/whitepapers/motivations of recent android malware.pdf, 2011. Last accessed November 9, 2017.
- Swendeman D, Rotheram-Borus MJ. Innovation in sexually transmitted disease and HIV prevention: Internet and mobile phone delivery vehicles for global diffusion. Curr Opin Psychiatry. 2010;23(2):139–44.
- Lester RT, Ritvo P, Mills EJ, Kariri A, Karanja S, Chung MH, et al. Effects of a mobile phone short message service on antiretroviral treatment adherence in Kenya. Lancet. 2010;376: 1838–45.
- Mitchell KJ, Bull S, Kiwanuka J, Ybarra ML. Cell phone usage among adolescents in Uganda: acceptability for relaying health information. Health Educ Res. 2011;26(5):770–81.
- Puccio JA, Belzer M, Olson J, Martinez M, Salata C, Tucker D, et al. The use of cell phone reminder calls for assisting HIVinfected adolescents and young adults to adhere to Highly Active Antiretroviral Therapy: a pilot study. AIDS Patient Care STDS. 2006;20(6):438–44.
- Jones, R and Lacroix, L.J. (2012). Streaming Weekly Soap Opera Video Episodes to Smartphones in a Randomized Controlled Trial to Reduce HIV Risk in Young Urban African American/Black Women. AIDS Behav. 16:1341–1358. DOI 10.1007/s10461-012-0170-9
- Doam CR, Portilla LM, Sayre MH. NIH conference on the future of telehealth: essential tools and technologies for clinical research and care—a summary, June 25–26, 2009 Bethesda, Maryland. Telemed J E Health. 2010;16(1):89–92.
- Ackerman, M.J., Filart, R., Burgess LP, Lee I, Poropatich RK. Developing next-generation telehealth tools and technologies: patients, systems, and data perspectives. Telemed J E Health.2010;16 (1):93–5.

- Muslukhov, I. (2012).Survey: Data Protection in Smartphones Against Physical Threats. Accessed at http://blogs.ubc.ca/computersecurity/files/2012/04/IMuslukhov_paper.pdf on November 9, 2017.
- McAfee Inc. The lost smartphone problem
- http://www.mcafee.com/us/resources/reports/rp-ponemon-lost-smartphone-problem.pdf.
- Mobile Africa (2015). Study reveals Ghana mobile phone usage stats. Accessed at http://citifmonline.com/2015/04/08/study-reveals-ghana-mobile-phone-usage-stats/ on November 9, 2017.
- C. Dagon, T. Martin, and T. Starner, "Mobile Phones as Computing Devices: The Viruses Are Coming," *IEEE Pervasive Computing*, vol. 3, no. 4, 2004, pp. 11–15.
- Yu, X., Wang, Z., Sun, K., Zhu, W.T., Gao, N., and Jing, J. (2014). Remotely Wiping Sensitive Data on Stolen Smartphones. http://dx.doi.org/10.1145/2590296.2590318.
- PC Magazine [Internet]. Definition of: smartphone. New York: Ziff Davis, Inc; 2011. Available from: http://www.pcmag.com/encyclopedia_term/0,2542,t=Smartphone&i=51537,00.asp
- Joe Wilcox. Two stories of smartphones stolen. http://www.oddlytogether.com/post/485601927/ two-stories-of-smartphones-stolen
- Seung-Hyun Seo, Dong Guen Lee, Kangbin Yim, "Analysis on Maliciousness for mobile application", IMIS 2012, pp. 126-129, 2012.7.
- P. D. Meshram and R.C. Thool (2014). A survey paper on vulnerabilities in android OS and security of android devices. IEEE. DOI: 10.1109/GCWCN.2014.7030873.
- Ghana Statistical Service, *Estimation of population in Ghana, Ghana, Accra, Ghana,* 2016. Accessed at http://www.statsghana.gov.gh/ on September 2, 2017.
- Carey JW. Linking qualitative and quantitative methods: Integrating cultural factors into public health. Qualitative Health Research. 1993; 3:298–318.
- Haiying Long (2014) An Empirical Review of Research Methodologies and Methods in Creativity Studies (2003–2012), Creativity Research Journal, 26:4, 427-438, DOI:10.1080/10400419.2014.961781
- Milne J (n.d.) Questionnaires: Some advantages and disadvantages. Center for CBL in Landuse and Environmental Sciences, Aberdeen University.
- Patton MQ (2002) Qualitative research and evaluation methods 3rd ed. Thousand Oaks, CA: Sage.
- Creswell J (2003) *Research design: Qualitative, quantitative and mixed methods approaches (2nd ed.).* Thousand Oaks, CA: SAGE Publications
- Androidcentral: 2016 http://www.androidcentral.com/google-says-there-are-now-billion-active-android-devices-worldwide
- Nathan Scrivens and Xiandong Lin (2017). Android Digital Forensics: Data, Extraction and Analysis. http://dx.doi.org/10.1145/3063955.3063981