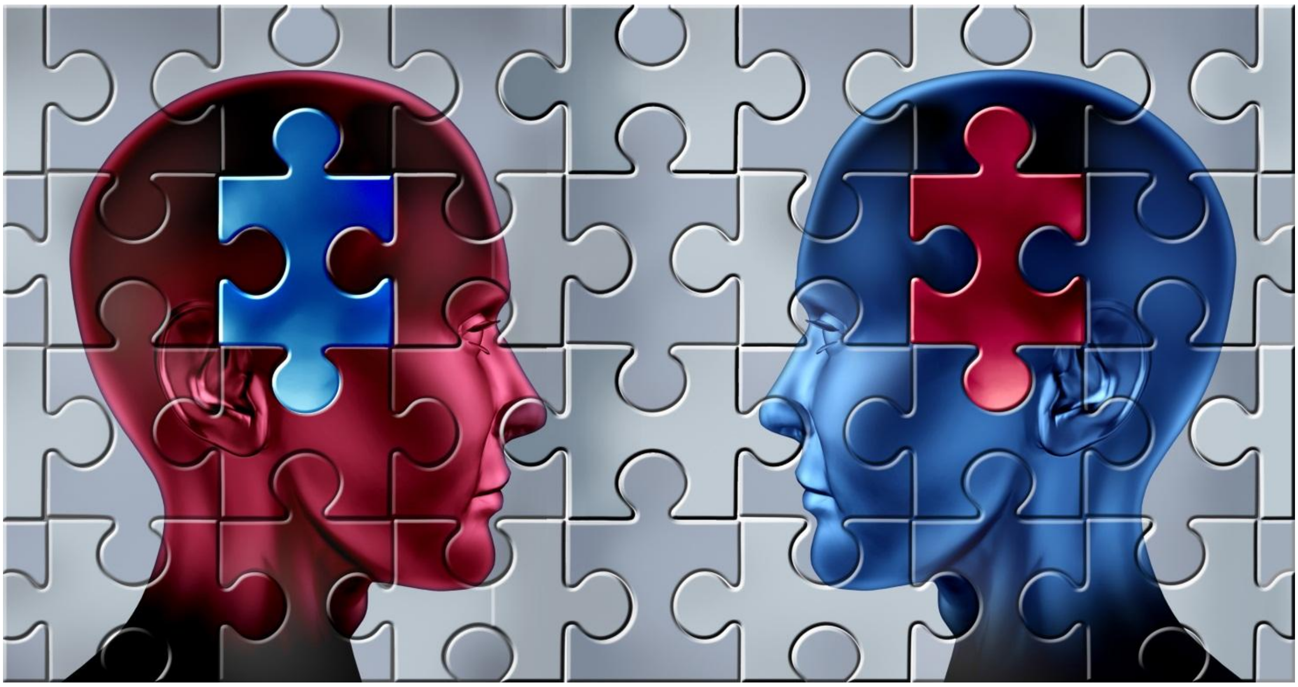

Exchanges: the Warwick Research Journal

Volume 2 (1), October 2014

http://exchanges.warwick.ac.uk

Learners' Perception on Security Issues in m-learning (Nigerian Universities Case Study)

Shaibu Adekunle Shonola and Mike S Joy

Learners' Perception on Security Issues in M-learning (Nigerian Universities Case Study)

Shaibu Adekunle Shonola and Mike S Joy (University of Warwick)

Abstract

With the advent of modern technology, mobile phones and smartphones are used not only for calling and text messages but also for banking and social networking. Recent developments in technology have made the use of mobile devices feasible in other sectors such as education and government. While educators are using mobile devices as teaching aids, students are also using them as learning tools. In some cases the developers of mobile learning in universities are making m-learning apps without serious consideration for security aspects whereas the handheld devices pose a serious threat to confidentiality, integrity and privacy of users including the learners. As a case study, this paper investigates the security concerns that students may have with the introduction of m-learning in higher education institutions in Nigeria and how this impacts on their learning. It examines the effects of security threats in m-learning on students and provides recommendations for alleviating these threats.

Keywords: mobile learning; m-learning; m-learning security; mobile device; handheld device; security issues.

Introduction

Traditional distance learning and e-learning have improved the quality of education by adding flexibility, comfortability and, at times, shortening the length of study (Beauchamp and Kennewell, 2010). While distance learning is mainly paper based, e-learning is a digital platform for passing knowledge from instructors to their students as well as a medium that eases information dissemination among them. e-learning is a method of educational delivery via electronic media to boost the learner's knowledge, and learning skills. With the advent of emerging mobile technologies and maturity in e-learning, the need to integrate mobile devices into learning is inevitable. Mobile-learning (m-learning) is an emerging innovation that is being integrated into distance and e-learning programmes to give a complete package of virtual education (Ozuorcun and Tabak, 2012). It is the delivery of educational material through mobile devices, such as personal digital assistants (PDAs), iPods, mobile phones, smartphones and tablets (Sitthiworachart and Joy, 2008).

The use of mobile devices in education is increasing due to the availability and affordability of mobile phones, smartphones and tablets. According to the Cisco report, by 2012, 7 billion mobile devices had been sold worldwide (Cisco, 2012). The main focus of m-learning is to utilise the substantial development in mobile technologies to the utmost advantage of the learners to improve their learning process and shorten the learning curve (Keegan, 2005). Another focal point of m-learning is to facilitate information sharing, which makes it possible for learners to interact with each other and share knowledge anytime. In an educational context, mobile phones are broadly used by students to access and support learning (Aderinoye et al., 2007) and many learners exploit the interactivity and sociability of web 2.0 technologies, such as wikis, online forums, blogs, image sharing and other social media in the area of arts and humanities.

M-learning also allows learners to communicate with their lecturers, as well as access learning content and resources, while on the move. Thus, students who use mobile technologies for learning are not only closer to their lecturers and tutors, but also in full control accessing learning content and instructions through their mobile devices. Therefore, one of the advantages of m-learning is that it gives learners a degree of liberty, freedom and independence in the course of learning (El-Hussein and Cronje, 2010). Although, Taleb and Sohrabi (2012) listed the educational uses of mobile devices by students to include; access to an online dictionary, message texting as well as for scientific calculations, the authors further attributed to Levy (2007) that students who use mobile technology devices have more motivation for learning than those who do not.

The use of mobile technologies by learners, however, has implications for security in term of integrity, confidentiality, and privacy of the users' data who are involved in the learning process. In this regard, learner records, e-portfolio data, assessment grades and feedback are some examples of sensitive information that need protecting when using mobile devices in education (Kambourakis, 2013). Therefore, the challenge is to safeguard what should be learnt in the lecture room, what should be learnt outside the classroom, and the methods in which connections between these two settings should be made (Hashemi *et al.*, 2011). The issues examined in this paper are loss or theft of mobile device, unauthorised access, attack on m-learning system and denial of service. Denial of service (DoS) is a form of attack in which users are deprived of the services of a resource they would normally expect to have. It is aimed at complete disruption of routing information which consequently affects the whole operation of wireless network and normally affects the availability of m-learning system. While these security challenges affect the use of mobile learning in Nigerian Higher Education Institutions (HEI) and the students' viewpoints on mobile devices for learning, this article examines the learners' perceptions on security issues that affect them in mobile learning.

The first section of this article is a review of related research on m-learning security. It summarises an existing study on m-learning security and evaluates the recommendations made in the literature. The second part discusses the research carried out on security issues that affect the use of m-learning in Nigeria from university students' perspective, and details the purpose of the research, the methodology and research questions. A brief overview of the analysis of the results of the research is presented in section three while section four gives a detailed discussion of the results gathered and statistical tests. The last part of this article highlights and discusses recommendations given to the security issues mentioned in the previous sections. The article concludes with problems encountered during the research and direction for future work in ensuring a robust and highly secure m-learning environment.

Literature Review

In as much as mobile devices have capabilities to motivate modern and innovative ways to learn; the security issues inherent in mobile devices are also transferable to m-learning. There are perceived risks, such as unauthorised interfering with the learning content and instructions. Educational institutions, educators and individual learners are also extremely concerned about the increasing threats to users' data security and privacy, since in most cases, learners are allowed to use their handheld devices to access learning content and materials. There are notable works on mobile learning and the learners' views on the use of m-learning, some of which are examined below.

Zamzuri *et al*.,(2013) state that students are the biggest users of any modern learning system and they are concerned about their privacy and security when using the system. Many learners are worried that their confidential information such as assessment results might be revealed to others. The authors propose that students' needs and views be considered in ensuring that the system is successfully implemented in any particular institution. Alwi and Ip-Shing (2009), who studied the perception of learners via e-learning (of which m-learning is a subdivision), found that there are security threats in the online learning systems, and that reliable security management in e-learning is significant in securing the modern learning environment. These studies are more peculiar to an e-learning environment and apart from privacy issues, they did not state other security threats being faced by learners when using mobile devices for learning.

In a study conducted in Nigeria, Boyinbode and Akinyede (2008) indicate that m-learning is the gateway to e-learning for many Nigerian students and it has already started to play a vital role in e-learning in Nigeria by bringing e-learning to students in rural communities. Adedoja *et al.*, (2012) stated that m-learning allows students to send and receive learning content that contains graphs, images, video and sounds, making it a platform to create reality and dynamism needed for effective learning. They remark that mobile technologies improve the productivity and efficiency of learners in Nigeria by delivering educational materials and support in real time and right context for their immediate needs, and conclude that having a good mobile technology infrastructure in the absence of other alternatives has made m-learning a good choice for Nigerian learners.

Osang *et al*., (2013), however, argue that many learners using the wireless internet without any supervision or monitoring might lead them to join negative groups on social networks, which might threaten their personal safety and the security of their mobile devices. They cite prevalent kidnapping cases in the country, as well as the recently publicised death of a Nigerian student who was killed by kidnappers in a hotel where they arranged to meet via social media, vividly emphasizing the potential grave dangers unassuming people are exposed to in the hands of those who abuse the technology.

The results of the study conducted by Alzaza and Yaakub (2011) in Malaysia show that students have satisfactory knowledge and good awareness of mobile technologies that may be used to enhance their learning experience. Similarly, the research conducted by

Rafiu *et al.,* (2011) shows that learners in Nigerian universities are well prepared for m-learning as they have various types of mobile devices in their possession and demonstrated high level usage skills for successful implementation. While the studies examined above are relevant because they discuss students' views on m-learning, they do not highlight any security challenges the students are facing when using their mobile devices for learning purposes. This article aims to assess mobile learning security from the students' perceptions and examine the risks that might affect m-learning in HEIs in Nigeria as well as the perceived damaging effects to the students in case of a security breach. Taking this approach will not only remove the concerns that students are having regarding the security of m-learning but also enable them to take full advantage of m-learning for their education.

Research Questions

The purpose of this study is to provide answers to the following questions.

(a) How important is the perceived security of m-learning devices to learners and why?

(b) What are the security concerns learners have when using mobile devices for learning?

(c) What are the perceived damaging effects of m-learning security threats to the students?

Methodology

This study employed a survey research approach using a sample population of students from three Universities in Nigeria. The data collection method involved delivering a set of questionnaires to 90 randomly selected students. The questionnaire comprised of 21 single and multiple choice questions divided into 4 sections. Section one was on demography and it collected personal information about the respondents. Questions in section two were concerned with the mobile devices used by the respondents and what type of activities they were being used for. Section three gathered data on m-learning awareness, the learning activities they were being used for and if m-learning improved their learning skills and performance. Section four was based on the security aspects of m-learning. It obtained information about the importance students placed on the security of their device(s), i.e. their security concerns about m-learning. In addition to the perceived threats being analysed, section four was designed to assess if the security of their mobile device had previously been breached, how it was breached and the effect it had on them. This section concluded with how mobile learning security issues can be assessed and minimised. Only the demographic and mobile security parts were used for analysis in this article.

The questionnaires were distributed at core lectures during the first semester of the 2013/2014 session after ethical consent was sought and obtained for the survey through the authors' university (BSREC approval REGO-2013-472), and respondents to the questionnaire were assured anonymity. The data collected was analysed and presented using frequency distributions, pie charts, histograms and statistical tests. Figure 1 illustrates a summary of the demographic distribution of the study participants; responses came from 42 females (46.67%) and 48 males (53.33%). The largest numbers of participants were students in the age group 20 – 25, which accounted for (60%).

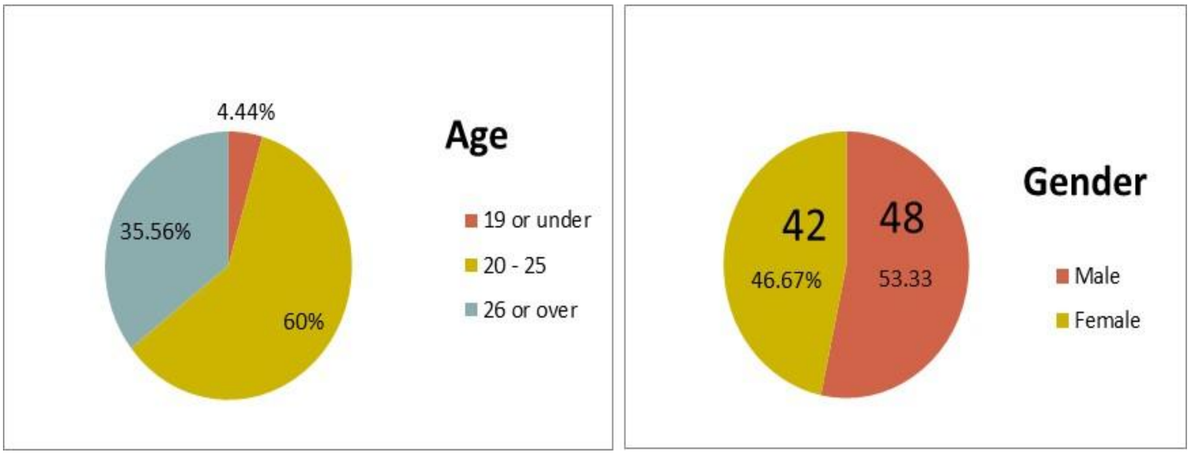

Figure 1: The demographic distribution of the study participants (N=90)

Results

The findings of this work are organised into three sections in order to provide answers to the research questions as shown below.

Research Question 1: How important is the perceived security of m-learning devices to students and why?

This is a single choice closed question to determine how important students consider the security and safety of their mobile phone, smart phone, tablets and other handheld devices to be. All the 90 students responded to the question. As shown in figure 2, two-thirds (65.56%) responded that the security of their device is 'very important' to them, 31.11% indicated it is 'important', and only 3.33% said it is 'neither important nor unimportant' to them. There were various reasons given by the participants as to why the security of their m-learning devices is important to them, some of which are highlighted in the discussion section of this article. Tables 1 and 2 show the percentage of the participants on demographic distribution. Based on a total scale of 100%, 44.45% and 52.22% of female and male students respectively said the security of their mobile device is 'important' or 'very important' to them. On the same scale for age groups, 3.33% of 19 and under, 57.78% of 20-25 and 35.56% of 26 and over said the security of their mobile device is 'important' or 'very important' to them.

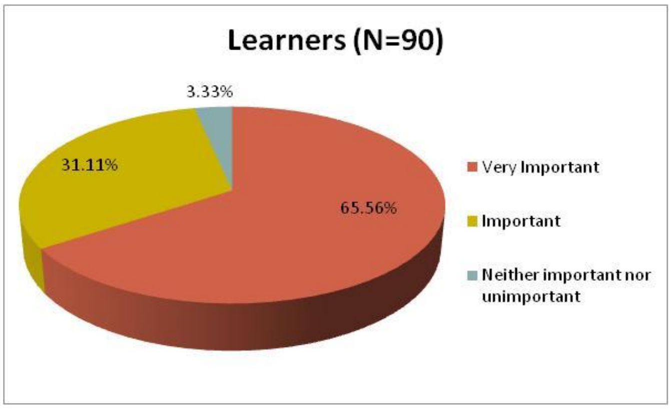

Figure 2: How important is the security of mobile devices to respondents

	Gender		Total (%)
	Female	Male	
Very important	25.56	40	65.56
Important	18.89	12.22	31.11
Neither important nor unimportant	2.22	1.11	3.33

Table 1: Demographic information on importance of security based on gender

	Age Group (%)		
	19 or under	20 - 25	26 and over
Very important	1.11	36.67	27.78
Important	2.22	21.11	7.78
Neither important nor unimportant	1.11	2.22	0

Table 2: Demographic information on importance of security based on age groups

Research Question 2: What are the security concerns students have when using mobile devices for learning?

This research question was designed to find out which security issues students are concerned about encountering when using their mobile devices for learning. Approximately four out of ten of the participants (42.27%) agreed that theft is a concern when using mobile devices for learning while over half of the respondents (54.43%) said loss of mobile device is a concern to them. 81.11% indicated that colleagues and friends are likely to use their handheld device without their permission, which is a concern that may lead to unauthorised access. Nearly seven out of ten of the participants (67.78%) thought that virus or malware attacks are inevitable when using a mobile device for learning while nearly a third of the participants (32.22%) said ‘denial of service’. These are shown in figure 3 below. Tables 3 and 4 show the demographic information on security concerns students may have on m-learning based on gender and age group, respectively.

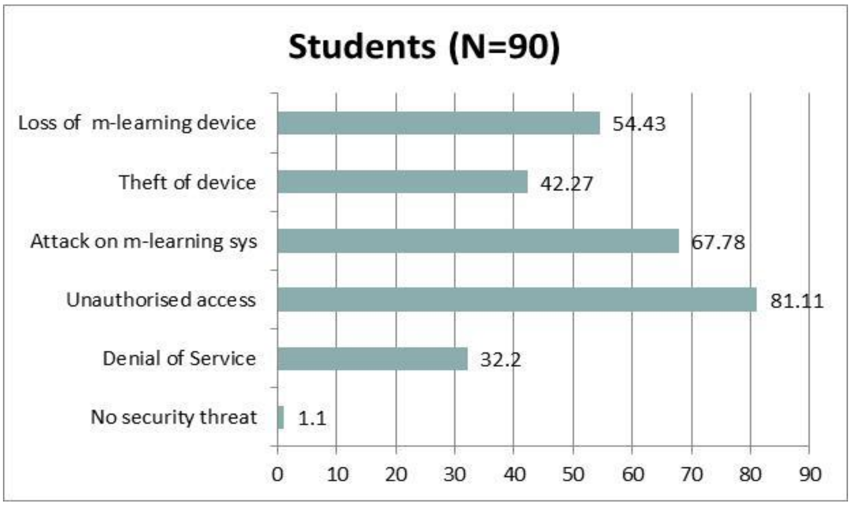

Figure 3: Security issues students might encounter in m-learning

	Gender		Total (%)
	Female	Male	
Theft of m-learning device	20	22.22	42.22
Loss of m-learning device	25.56	28.89	54.45
Malware/ Virus attack	30	37.78	67.78
unauthorised access	34.44	46.67	81.11
Denial of Service	15.56	16.67	32.23
No Security threats	1.11	0	1.11

Table 3: Demographic information on students’ security concerns based on gender

	Age Group (in %)		
	19 or under	20 - 25	26 and over
Theft of m-learning device	1.11	26.67	14.44
Loss of m-learning device	3.33	32.22	18.89
Malware/ Virus attack	4.44	34.44	28.89
unauthorised access	2.22	45.56	33.33
Denial of Service	4.44	23.33	4.44
No Security threats			1.11

Table 4: Demographic information on students' security concerns based on age group

Research Question 3: What are the perceived damaging effects of m-learning security threats to the students?

Figure 4 shows the most common concerns of students on the perceived effects of m-learning security in the universities surveyed. A large numbers of the participants said they are likely to suffer loss of confidential or personal information in the event of security breach. This view accounted for 92.22% of the participants. Loss of study hours and loss of performance accounted for 72.22% and 75.56% respectively. Psychological effects resulting from security breaches of mobile devices accounted for 50% while two people indicated that they are not likely to experience any damaging effects as a result of security breach. Tables 5 and 6 show the demographic information on the perceived damaging effects of security breach based on gender and age group respectively.

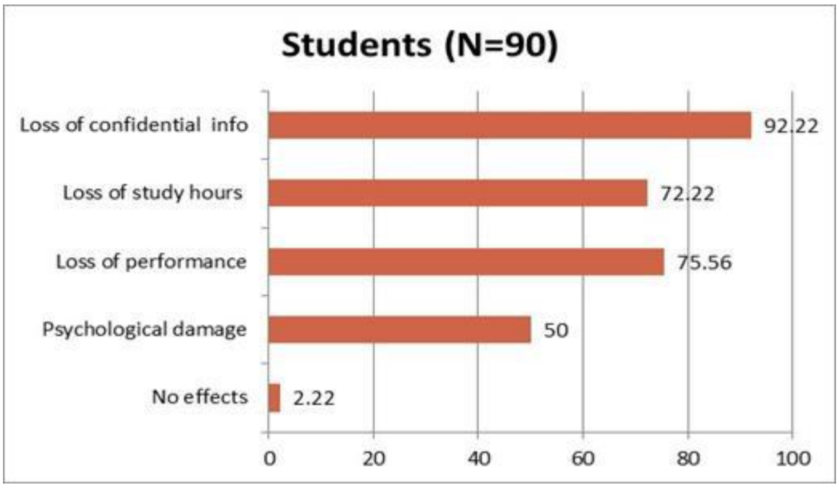

Figure 4: Damaging effects of m-learning security threats to students

	Gender (in %)		Total (%)
	Female	Male	
Loss of confidential info	43.33	48.89	92.22
Loss of study hours	32.22	40	72.22
Loss of performance	33.33	42.22	75.56
Psychological damage	21.11	28.89	50
No effects	1.11	1.11	2.22

Table 5: Demographic information on security effects based on gender

	Age Group (in %)		
	19 or under	20 - 25	26 and over
Loss of confidential info	4.44	56.67	31.11
Loss of study hours	2.22	41.11	28.89
Loss of performance	4.44	42.22	27.78
Psychological damage	2.22	28.89	18.89
No effects	0	1.11	1.11

Table 6: Demographic information on security effects based on age groups

Discussion

Figure 2 shows how important students take the security of their mobile devices. Cumulatively, almost all the respondents agreed that the security of their mobile devices is ‘important’ to them. This result suggests that many students take the security of their mobile devices seriously. Many reasons are given by the students for taking the security of their mobile device seriously, the first reason being that mobile phones and smartphones are considered to be valuable personal property, consequently they attempt keep them safe. Many learners use their handheld devices to exchange education-related messages and learning contents with classmates, search the internet and library databases for learning materials, and hold group discussions with classmates. Therefore, they believed that their mobile devices are vital to their academic success and they are mindful of the security of their mobile devices. Furthermore, many students also use their handheld devices as data storage, thus they have their personal information on them. Consequently, having mobile security awareness is an important aspect of protecting their privacy. This result is supported by the work of Kambourakis (2013) that discusses the security and privacy challenges of m-learning and suggests that learners are extremely concerned about the security and safety of the data they store on their mobile devices.

This result was further analysed using the chi-square statistical test for dependency based on the demographic information. The chi-square statistic was calculated to be 4.1017, the P-value - 0.128627, and confidence interval of 0.050. The test shows that there is no gender difference on how important the security of m-learning devices is. However, for the test performed on age group, the chi-square statistic is 10.284; P-Value - 0.035906 and the same confidence interval of 0.050. The statistical test shows that there is a significant difference on how important the security of m-learning device is based on age group. This statistical test implies that students tend to be security conscious about their mobile devices based on their age.

Figure 3 relates to perceived security issues students may encounter when using mobile devices for learning. A very high percentage of students (81.11%) perceived the unauthorised use of portable devices by friends or classmates of the owners as a security risk. The potential for unauthorised use of portable devices is suggested to be high among learners in Nigeria since they usually live in shared hostels; mobile devices left on a table can be picked up by roommates and used for gaming or educational purposes. This act may lead to unauthorised access to confidential information of the owner since many students have personal details such as full name, address, date of birth, email address and even their bank account information on apps on their mobile devices.

Significant proportions of the perceived risks are loss and theft of mobile devices. These are common in many developing countries since mobile devices are still regarded as precious possessions and in some cases where the HEI supplies learners with mobile devices, there are concerns about making learners attractive to thieves. This result is in line with Obodoeze *et al.'s*(2013) study which demonstrated the second most challenging security concerns affecting mobile users in Nigeria is the frequent or widespread losses of mobile device by their owners to thieves or the owners carelessly lose their mobile phones while in transit. Virus and malware attack is also perceived as a threat when using handheld devices for learning purposes and they are normally encountered when downloading educational materials from an unknown source. This result is also consistent with the work of Obodoeze *et al.*, (2013), which identifies the various forms of threats including virus/malware attack and hacking as the biggest security challenges being faced by mobile device users in Nigeria.

Access to information, group discussion as well as learning content and instructions may be disturbed through DoS if the network is penetrated. In addition, it is a threat that results from irregular power supply to mobile learning servers, which is common in developing countries. This study is supported by the findings of Osang *et al.*,(2013) in which 64% of the respondents identify that the poor power supply situation in the country is a barrier tom-learning. Furthermore, DoS may occur during scheduled or unscheduled downtime due to maintenance of network infrastructure, which can lead to loss of connectivity between mobile devices and servers. It can also be caused by physical attacks on network infrastructure on universities campuses, which are common, for example during student riots in some universities in developing countries such as Nigeria.

A statistical test for observable gender differences linked to the perceived students' security concerns were carried out using nonparametric Mann-Whitney U Test. The U-value was calculated as 15 and the critical value of U - 5. Therefore, statistically significant gender difference does not exist at confidence interval of 0.050. Similarly, a test for observable age group differences linked to the perceived security concerns were carried out using Kruskal-Wallis Test for age group; there was no statistically significant age group difference at confidence interval of 0.050.

Figure 4 analyses the perceived damaging effects to the students in the event of a security breach. 92.22% of the learners agreed that loss of confidential information is the most hurtful effect. This result is consistent with the work of Zamzuri *et al.*, (2013), which states that one of the reasons why students reject online systems is due to security reasons because they are worried about the loss of their private and confidential information. The study also reveals that 70% of learners' feared loss of study hours and performance as consequences of a security breach in m-learning due to DoS, which is possible when learners view m-learning systems as a complement to the classroom and rely on it as one of their main learning platforms. This implies that non-availability for a long period of time will have adverse effects on learners' study hours, revision time and consequently their performance. This finding is in line with the work of Kukulska-Hulme *et al.*,(2009),which states that good m-learning improves learners' study retention and performances in their study. Therefore, learners need a reliable, highly available and dependable m-learning system to avoid being frustrated in the event of disconnection to the m-learning system, which can affect their study performance adversely. This raises the worry that students may be reluctant to fully engage with m-learning and therefore fail to realise the full potential of m-learning to their learning experience because of their concerns about loss of study hours and performance in the event of a security breach.

Half of the learners believed that they are likely to experience psychological disturbance if their personal information is leaked through a mobile device or m-learning system or if their privacy is infringed.

In uniformity with other research questions, the result was further analysed using chi-square (5 x 5 table) statistical test for dependency based on the demographic information and age group. The chi-square statistic was calculated as 0.3166, the P-Value - 0.988718and confidence interval of 0.050 for the gender demography. For age group, chi-square statistic was calculated as 1.3706, the P-Value - 0.994653 at confidence interval of 0.050. Both tests, therefore show that there are neither gender nor age produce significant differences in the damaging effects felt by the students in the event of an m-learning security breach.

It should be noted that responses of the participants are limited to their experience and knowledge about m-learning and security issues surrounding m-learning environments as well as their mood when completing the questionnaire. The participants were asked to respond to the questions as practically as possible and to answer the questionnaire based on their view on m-learning.

Recommendations

Having discussed the issues pertaining to m-learning security as well as the damaging effects from learners' viewpoints, it is important to highlight possible suggestions and put in place strategies for alleviating these perceived security issues relating to m-learning systems, starting from the mobile devices and including the servers and network infrastructure, by engaging proper security procedures and policies.

The first task in alleviating security issues in relation to students' perceptions' of m-learning is to create awareness and information education about mobile security. This is imperative as our study revealed that, while most of the students considered the security of their mobile devices as very important or important, some of them do not. With adequate knowledge, learners will be more security conscious about the safety of their handheld devices. Being security conscious will make learners take proper care for their devices and help to alleviate their concerns of loss or theft of their device.

Similarly, security consciousness should be encouraged among learners who connect to educational resources while on the move using any free available WI-FI. While some students may not consider connection to free WI-FI a major security threat, in some cases it may pose significant risk and there is need to educate them on the dangers. Furthermore, they should be aware of the credibility of the organisation providing the connection regarding the security and safety of free network facilitates before using it. For example, connecting to an unsecured and unverified wireless infrastructure increases the chances of putting personal data at risk. Therefore, students should take note of the potential risks of automatically connecting to unknown free wireless access points, which may be intercepted or controlled by attackers and may lead to unauthorised access to their mobile device and learning materials stored in it.

Overcoming unauthorised access is possible by having robust access control mechanisms for authentication and authorisation before permission is given to access the device or view learning content and materials. Password lock or biometric access will prevent other learners from using the device if left on the table by the owner. Meanwhile, mobile devices will not be left on the table unattended if the owner is security conscious as mentioned earlier. Devices like mobile or smart phones should remain in owners' pockets when not in use while tablets should be kept away. Similarly, encryption of data on m-learning devices will further safeguard learning content, student's personal information, assessment records and grades from unauthorised access if lost or stolen. While students' personal details, assessment records and grades are required to be safeguarded for confidentiality and privacy reasons, learning contents are needed to be safeguarded for copyright protection purposes, unauthorised access and against manipulations which have been identified as security issues in e-learning (Graf, 2002) as well as m-learning.

DoS can be overcome by putting in place scheduled maintenance policy for m-learning servers and network infrastructure as well as an uninterruptible power supply. DoS resulting from network breach can be avoided using prevention techniques for counteracting DoS such as protocol traceback techniques on the m-learning servers (Tupakula and Varadharajan, 2013) and reverse proxies spread across multiple hosting locations.

The recommendation for alleviating perceived security issues on virus and malware attack is the use of legacy protection mechanisms. This involves having regular data backup, installing firewalls and having up to date anti-malware and anti-virus software installation on m-learning devices. Furthermore, all interfaces including Bluetooth interface should be highly secured. For example, mobile firewalls normally inspect IP interfaces, but they often overlook the Bluetooth interface (Razaque and Elleithy, 2012).

Conclusion and further research

This article discusses learners' perceptions on security aspects of mobile learning, which is expanding the possibilities of open and distance learning education. Students are willing to embrace their use of mobile devices for learning purposes not only to augment classroom lectures but also to achieve the globalisation objective (Hashemi *et al.*, 2011). Their interest and expertise are of great potential for m-learning if integrated into their learning curriculum (Dale and Povey, 2009). However, the security and confidentiality of their private information being exposed in the process of m-learning are of great concern to them, which may lead to a reluctance to use such technology and consequently fail to realise the full potential of m-learning. Therefore, provision of robust mechanisms to support learners' authentication, authorisation, content copying and downloading, and safeguarding learner examinations, assessment and feedback processes from attackers and impostors are what the learners want in an m-learning environment.

Student records, e-portfolios and faculty data are some of the confidential information that need to be protected while students' privacy should be guaranteed at all times (Luminita and Magdalena, 2012).Adequate security measures are required to ensure that highly secured connections are maintained between the learners' devices and m-learning servers by deploying proper security policies and measures so as to deter and repel attacks. Similarly, learners should ensure that they connect their devices only to trusted and tested networks in order to safeguard data transferred during the m-learning process.

They should avoid downloading learning materials from illegitimate sites which are common sources for malware attacks.

In conclusion, mobile learning is going to increase in patronage as technology advances, the security issues in mobile devices which are also on the increase are transferable to m-learning systems. Learners are most highly likely to be affected since they are the main users of m-learning. Therefore, adequate security education and awareness inform of tutorials and tips should be put in place for the learners in order to minimise the security palaver and give them confidence in using such technology.

This article considers m-learning security from learners' perspectives, our previous publication discusses m-learning security from lecturers' perspectives (Shonola and Joy, 2014). However, there are still many grey areas in m-learning security where limited or no research has been done, such as common attack routes in m-learning security breaches, collective responsibilities of m-learning stakeholders in combating security breaches and other perceived threats to m-learning in developing countries apart from security. Therefore, future research work should focus on these areas.

References

Adedoja, G., Botha, A., and Ogunleye, O.S. (2012), 'The Future of Mobile Learning in the Nigerian Education System', *IST-Africa 2012 Conference Proceedings Paul Cunningham and Miriam Cunningham (eds) IIMC International Information Management Corporation, 2012*

Aderinoye, R.A., Ojokheta, K.O. and Olojede, A.A. (2007), 'Integrating Mobile Learning into Nomadic Education Programmes in Nigeria: issues and perspectives', *International Review of Research in Open and Distance Learning,* 8(2), 44-52

Alwi, N. M, and Ip-Shing, F (2009). 'User's Perception in Information Security Threats in E-Learning', *Paper presented at the 2nd International Conference of Education, Research and Innovation. ICERI2009 Proceedings, Madrid, Spain*. pp. 2345-52

Alzaza, N.S. and Yaakub, A.R (2011) 'Students' Awareness and Requirements of Mobile Learning Services in the Higher Education Environment', *American Journal of Economics and Business Administration*, 3(1) 95-100

Beauchamp, G and Kennewell, S. (2010) 'Interactivity in the classroom and its impact on learning', Computers & Education, 54(3), 759-766

Boyinbode O. K. and Akinyede R. O.(2008) 'Mobile Learning: An Application of Mobile and Wireless Technologies in Nigerian Learning System',*International Journal of Computer Science and Network Security*, 8-11.

Cisco, 'Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2011–2016', 14 February 2012, Available online http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html accessed 11June 2014

Dale, C. and Povey, G. (2009),'An Evaluation of Learner-Generated Content and Podcasting', *Journal of Hospitality, Leisure, Sport and Tourism Education*. Available from http://www.heacademy.ac.uk/assets/hlst/documents/johlste/vol8no1/PP0214Format117to123.pdf accessed 20 April 2014

El-Hussein, M. O. M. and Cronje, J. C. (2010), 'Defining Mobile Learning in the Higher Education Landscape', *Educational Technology & Society*,13(3)12–21.

Graf. F (2002), 'Providing security for eLearning', *Computers & Graphics*,26(2)355–65.

Hashemi, M., Azizinezhad, M., Najafi, V and Nesari A, J (2011). 'What is Mobile Learning? Challenges and Capabilities', *Procedia Social and Science Behaviour*,30, 2477– 81

Kambourakis, G (2013), 'Security and Privacy in m-learning and beyond: Challenges and state of the art', *International Journal of u- and e- services, Science and Technology*, 3-6

Keegan, D. (2005). 'The incorporation of mobile learning into mainstream education and training'. *World Conference on Mobile Learning, Cape Town*, October 2005.

Kukulska-Hulme, A., Sharples, M., Milrad, M., Arnedillo-Sánchez, I. and Vavoula, G.(2009), 'Innovation in Mobile Learning: A European Perspective' *,International Journal of Mobile and Blended Learning.* 1(1)13-35.

Luminita, C. D.C. and Magdalena, C.I.N (2012), 'E-learning Security Vulnerabilities', *Procedia - Social and Behavioral Sciences,* 46, 2297 – 301

Obodoeze, F.C., Okoye, F.A., Mba, C.N., Asogwa, S.C. and Ozioko., F.E (2013), 'A Holistic Mobile Security Framework for Nigeria', International Journal of Innovative Technology an Exploring Engineering (IJITEE) , 2 (3)1-11

Osang, F.B., Ngole, J., Tsuma, C (2013), 'Prospects and Challenges of Mobile Learning Implementation in Nigeria. Case Study National Open University of Nigeria NOUN' *International Conference on ICT for Africa 2013,* February 20-23, Harare Zimbabwe

Ozuorcun N,C and Tabak, F. (2012). "Is m-learning versus E-learning or are they supporting each other." Procedia Social and Science Behaviour. 46 (2012) 294-305

Rafiu, M.I, Kayode,S.A and Rapheal, T.O (2011),'Implementing Mobile-Learning in Nigeria Tertiary Educational System – A Feasibility Study, *International Journal of Science and Advanced Technology*1(1)7

Razaque, A and Elleithy, K (2012), 'Discovery of Malicious Attacks to Improve Mobile Collaborative Learning (MCL). *International Journal of Computer Networks & Communications (IJCNC),* 4(4).

Shonola, S.A and Joy, M.S. (2014), 'Mobile learning security issues from lecturers' perspectives (Nigerian Universities Case Study)'. *6th International Conference on Education and New Learning Technologies,7-9 July, 2014, Barcelona, Spain. pp.7081-88*

Sitthiworachart, J. and Joy, M.S. (2008), 'Is Mobile Learning a Substitute for Electronic Learning?' In proceedings of: IADIS International Conference e-Learning 2008, Amsterdam. pp. 451 – 458

Tupakula, U and V. Varadharajan (2013). 'Security Techniques for Counteracting Attacks in Mobile Healthcare Services'. The 3rd International Conference on

Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH-2013). Procedia Computer Science, vol. 21, pp. 374 – 81

Taleb, Z and Sohrabi, A. (2012), ‘Learning on the move: The use of mobile Technology to support learning for University Students’, *Procedia Social and Science Behaviour,*69,1102 – 09.

Zamzuri, Z. F., Manaf, M., Yunus, Y., and Ahmad, A. (2013),‘Student Perception on Security Requirement of e-Learning Services’, *Procedia-Social and Behavioral Sciences*. *90*,923-30.