A Digital Storytelling Model for Increasing Information Security Awareness among Kenyan Smartphone Users

***Kosgey Lynet.*[1*], *Mbogo Chao* [1], *Nyaga Mwaniki* [2]**

[1]*Kenya Methodist University, P.O. Box 45240-00100, Nairobi, Kenya.*
[2]*KamiLimu, Nairobi, Kenya*

**Correspondence email:* kosgeylynet@gmail.com

Abstract

The proliferation of smartphones in Kenya has resulted to smartphone users' overdependence on their phones for everyday activities. This increased interaction with smartphones poses a threat to users' privacy and security. The exposure to threats establishes a need to understand users' security awareness and behavior when using their mobile phones. To investigate user behaviour while using their mobile phones and their understanding of cyber security risks, this study surveyed 393 Kenyan smartphone users on security features that they implement as well as their understanding of potential security threats. The results show that most Kenyan Smartphone users are aware of security threats facing them and are greatly concerned about related security risks. However, users still make poor behavioral choices related to the use of smartphones, making them vulnerable to cyber security attacks. This paper proposes a Digital Storytelling (DST) model that forms a basis of creating a digital storytelling media that can be used to increase cyber security awareness among Kenyan smartphone users.

Keywords: *Information security, user awareness, cyber security, digital storytelling, Smartphone awareness, security training*

IJPP 8(1), 92-104

1.0 Introduction

The mobile penetration rate in Kenya is 97.8% (Communications Authority of Kenya [CAK], 2018), partly as a result of the rise of a youthful population in Kenya, which has seen the demand for smartphones going up and the price of smartphones dropping (Jumia, 2019). This increased interaction with smartphones poses a threat to users' privacy and security, with cybercrime listed as an emerging threat (Kiboi, 2015). Indeed, an increased rate of cybercrime and cyber-attack cases have been reported to the police (Serianu, 2018). Further, the cost of Cybercrime through mobile phones in 2017 was reported at 25 Million Kenya Shillings (Serianu, 2017).

This study surveyed 520 Kenyan smartphone users to understand the security countermeasures that they utilize, and their awareness of potential security threats while using mobile phones. The results show that most Kenyan Smartphone users are aware of security threats facing them and are greatly concerned about related security risks. However, users still make poor behavioral choices related to the use of smartphones; hence, making them vulnerable to cyber security attacks. Therefore, increasing information security awareness with the objective of impacting behavioral change has to be more than providing information to users – it has to be targeted, actionable, doable and provide feedback (Bada, et al., 2015). This paper aims to address this need.

The most preferred approach to address mobile security awareness among Kenyans is through media campaigns in the form of print, electronic, and social media (Okuku, et al., 2015). The effect of electronic media has been seen in the form of digital storytelling, which has been used to increase cyber security awareness among teachers (Khalid & El-Maliki, 2020).

Thus, a digital storytelling model could be adopted to increase information security awareness among Kenyan smartphone users.

The objectives of this paper were:

(i) To investigate user behaviour while using their mobile phones and their understanding of cyber security risks.

(ii) To design a digital storytelling model using existing frameworks and the identified behavioral gaps among smartphone users.

Smartphone user's security and privacy-related decisions are influenced by their attitudes, perceptions, and understanding of various security threats (Alsaleh, et al., 2017). Yet, in some cases users tend to ignore security measures even when they are aware of risks involved. For example, over 65% of smartphone users are concerned about their privacy and security although they continue practicing risky activities like giving application permission to access their data (Symantec Corporation, 2015). Unfortunately, lack of awareness of security measures and behavior that increases privacy and security risk saw five East African countries lose 245 Million dollars to online fraud (Quarshie & Odoom, 2012).

One approach that has been used to increase the awareness of information security is through experience sharing. For example, users reported that they would change their behaviour based on the security stories they had heard; especially if the stories had a serious lesson or if it was from knowledgeable sources (Rader, et al., 2012). A form of experience sharing utilizes digital media in the form of digital storytelling, which is the combination of a variety of digital multimedia, such as images, audio, and video to tell stories (Robin, 2011).

Digital storytelling has been used to develop awareness on online cyber risk such as internet addiction, pornography, game addiction and

bullying, among 10 to 14-year-old's (Khalid & El-Maliki, 2020). Further, it has also been used in an organization to form an effective information security culture, motivating employees, building a positive image and controlling crisis (Arsenijevic et al., 2016). Indeed, the advantage of storytelling is that apart from its instant behavioural change, it has the highest retention rate (Skinner et al., 2018)**.**

Digital Storytelling has also been used to impact knowledge in nursing (Clisbee et al., 2019) and in higher education to enable students to improve communication and idea creation (Clisbee et al., 2019).In addition , Digital Storytelling has been utilized in rural Africa to create applications that gather data in storytelling (Chan et al., 2017).

There are three types of digital stories: (i) historical documentaries that describe past events; (ii) personal narratives in which the authors express personal experiences; and (iii) stories that inform or instruct the viewer of a particular content (Robin, 2008)**.** This paper designs a digital storytelling model that informs smartphone users on information security practices.

Seven elements have been cited as contained in digital storytelling (Center for Digital Storytelling, 2005); namely, (i) the point of view, which describes the view of the author; (ii) a dramatic question that will be answered by the end of the story; (iii) emotional content that addresses an issues in a personal way; iv) the gift of your voice that contextualizes the story; v) the power of the soundtrack that is music or other sounds that support the story; vi) economy that refers to using brief enough content to tell the story without overloading the viewer; and vii) pacing the story so it neither progresses too slowly or too quickly. This research implements all these seven aspects.

2.0 Materials and Methods

Participants

To show gaps in behavioral choices that increase cyber security risks among Kenyan smartphone users, 520 individuals were surveyed from Nairobi and Eldoret cities in Kenya. The formula below was used to calculate the sample size.

$$\text{Finite population: } n' = \frac{n}{1+\frac{z^2 \times \hat{p}(1-\hat{p})}{\varepsilon^2 N}}$$

where
z is the z score
ε is the margin of error
N is population size
p̂ is the population proportion

This calculation is considering a confidence interval of 95%. Where z or 95% confidence level is 1.96 and population proportion of 0.5. Thus, the sample size was expected to be at least 384 random smartphone users, to reduce bias. 430 participants took part in the survey. The demographics are as shown in Table 1. There was almost a 50-50 representation of male and female participants. The age group with a higher representation was between the age of 20 and 30 at 53 percent, followed by 30-40 years with a percentage of 30 percent. Additionally, 71 percent.

Table 1

Demographics

Characteristics	Category	Overall	Percentage
Gender	Male	198	50%
	Female	187	48%
	Prefer not to answer	7	2%
	Not responded	1	0%
Age Group	Less than 20 years	4	1%
	20-30 years	219	56%
	30-40 years	113	29%
	40-50 years	32	8%
	Above 50 years	15	4%
	Prefer not to answer	9	2%
	Not responded	1	0%
Profession	Employed	286	73%
	Student	65	17%
	Retired	1	0%
	Unemployed	35	9%
	No answer	6	2%
Phone Operating System	Android by Google	344	88%
	IOS by Apple	33	8%
	BlackBerry	2	1%
	Windows Phone	3	1%
	I am not Aware	5	1%
	Not responded	6	2%
Phone Monitored by employer	Yes	20	5%
	No	372	95%
	Not responded	1	0%
IT Knowledge	Good	90	23%
	Moderate	159	40%
	Excellent	131	33%
	knowledge	12	3%
	Not responded	1	0%
Settlement Setting	Rural	51	13%
	Urban	340	87%
	Not responded	2	1%
Smartphone Ownership	Yes	392	100%
	No	1	0%
Country	Kenya	393	100%

percent of the participants were working or self-employed, with 18 percent as students. The participants also used android smartphones and displayed moderate to excellent Information Technology (IT) knowledge, with only 3 percent without IT knowledge. Finally, the majority of the participants lived in urban areas in Kenya.

The demographic representation of the participants confirms the ownership of smartphones among a youthful, urban population. The possession of IT knowledge among participants is relevant to this research in relating it to the knowledge and adherence to information security guidelines.

Data Collection

An online questionnaire was chosen as it can be used to reach many respondents irrespective of their geographical location. The questionnaire was designed using Google forms and consisted of two parts: (i) demography; and (ii) user awareness on information security practices. These sections were consistent with the objectives of this paper. Offline questionnaires were also utilized where the questions were printed for any user who had no access to the internet.

To alleviate any potentially ambiguous questions, a pilot survey was conducted on 20 individuals. This process was important to validate the survey by soliciting feedback and ensure that respondents would not have problems in answering questions and also to eliminate ambiguity. After the pilot survey, a total of 520 questionnaires were sent out by sharing a Google form link via email, WhatsApp, and printing the form. Of the 520 questionnaires sent out, 430 smartphone users responded. These responses represent 83% response rate. Of the 430 responses, we analyzed 393 users (91%) and discarded 37 responses as they were either incomplete or did not meet contextual criteria for target population.

The survey contained questions categorized into two sections. The first section was on user demographics that asked users their gender, age group, profession, IT Knowledge and the type of setting they live in. The second section

sought to understand device ownership and information security awareness.

Data Analysis

The data collected using the form was converted to a spreadsheet. The data was then cleaned using Microsoft Excel. Data cleaning involved identifying and correcting the inaccurate record. The data contained a mixture of qualitative and quantitative research. Data was then represented through text, graphs and tables.

User behaviour and their understanding of cyber security risks

To understand user behavior when utilizing smartphones, two issues were investigated: (i) security features utilized by smartphone users; and (ii) user awareness of potential security threats. Security measures are features that can be utilized by smartphone users to protect themselves. These features include phone update, phone locking, installing trusted application prompts among others. This research investigated which of these features were used by participants in order to identify gaps in the use of security features. To further understand user behavior, participants were asked about their awareness of security threats. This information would be useful in creating an effective information security awareness model using digital storytelling.

Digital Storytelling Framework

Table 2 shows a summary of the characteristics and processes that are used in this paper to design a digital storytelling model (DSM) for increasing cyber security awareness among Kenyan smartphone users.

Table 2

Characteristics and process framework for designing the digital storytelling model

Type of Digital Story	Characteristics of Digital Story	Process of designing the Model
Information-based	a) Point of view b) A dramatic question c) Emotional content d) Context e) Soundtrack f) Economy g) Pacing	a) Choose story characters b) Choose story language c) Choose narration style d) Select multimedia elements e) Develop story content f) Create the digital story g) Collect participants' feedback

(i) The DSM will be to inform the viewer (Robin, 2008**).**

(ii) The DSM will implement the seven elements contained in digital storytelling (Center for Digital Storytelling, 2005) in the following ways:

a) point of view, which will consider the results of the security features utilized by the users and also their knowledge of security risks and mitigations.
b) a dramatic question that will be answered by the end of the story, which will emanate from the most prominent issues that need increased awareness.
c) emotional content that addresses an issue in a personal way by identifying qualities of the study participants.
d) the gift of voice that contextualizes the story within the Kenyan context.
e) the use of soundtracks that support the story.

f) creation of the story within an economical time so as not to overload the viewer.
g) pacing the story so that it neither progresses too slowly or too quickly.

(iii) The DSM will follow a process used by teachers so as to create digital storytelling for cyber-risk awareness (Khalid and El-Maliki, 2020). However, these steps will not be followed in a strict order since some steps work best when completed together.

a) Choose story characters by considering the demographics of the participants involved in this study as well as information security experts.
b) Choose story language by considering the demographics of the participants involved in this study.
c) Choose narration style as either first-person or third-person narration.
d) Select multimedia elements such as software, soundtrack, images, text, audio.
e) Develop story content by writing a script. The content will relate to information obtained on user behaviour and understanding of cyber security risks.
f) Create the digital story that lasts for an economical time.
g) Measure the effectiveness of the digital story to increase cyber security awareness.

3.0 Results and Discussions

Security Features Utilized by Users

Figure 1 shows that 82% of the participants utilize Personal Identification Number (PIN) and fingerprint on their phones, and also 52% back up their data. This may also be because people often use PIN or password to access bank accounts, emails, and mobile service

Figure 1

Security features utilized by smartphones users

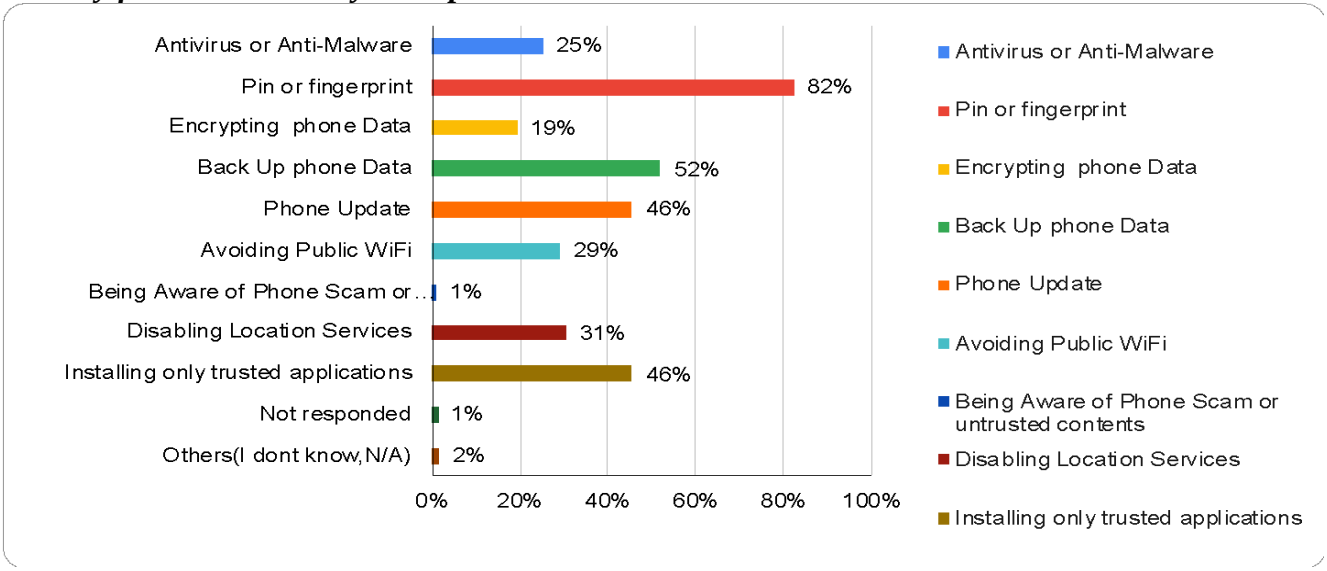
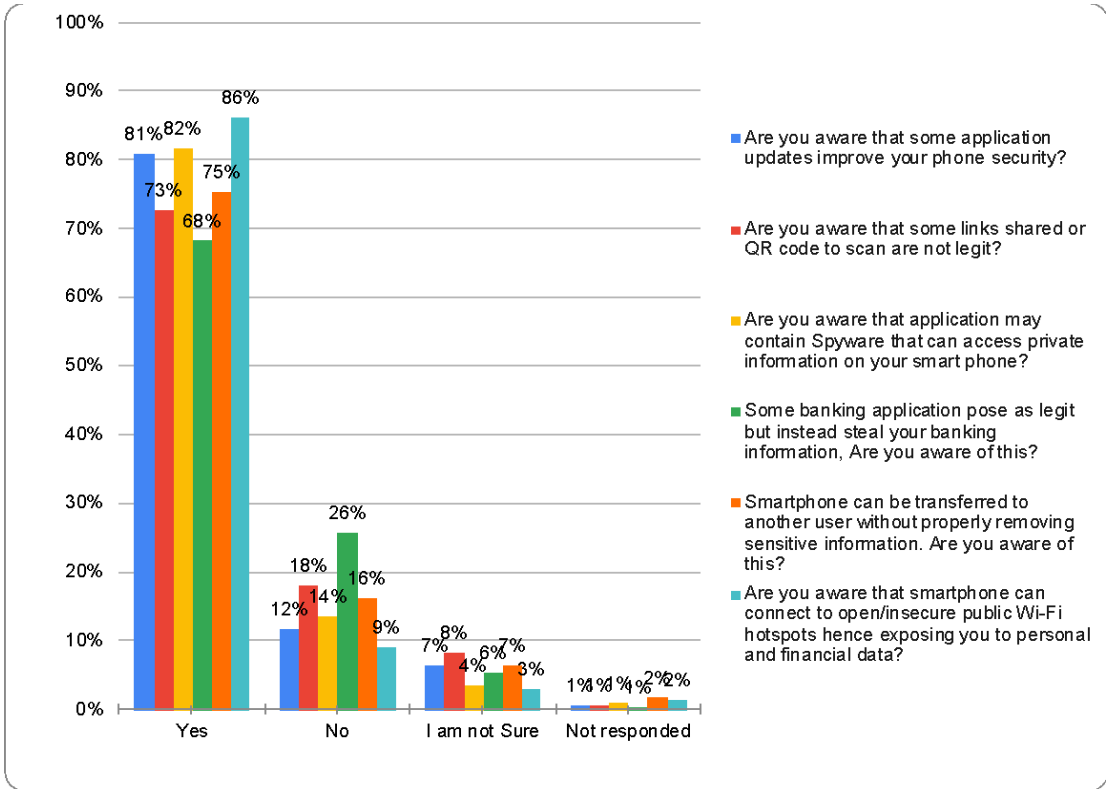


Figure 2

Awareness level of Security Risks



Providers. Further, social media, radio, or TV advertisement often reminds users of such security measures. For example, this advertisement by Safaricom, one of Kenyan's telecommunication firm, leading in mobile money market share, emphasizes on the use of voice as subscribers password to access its services (Safaricom PLC, 2018). On the contrary, less than 50% of the participants take security measures. For example, only 29% avoid the use of public unsecured WiFi, only 25% utilize antivirus, and just 19% encrypt their phone data. Also, while almost 50% of the users update their phone's software data and install applications from only trusted sources, they ignore other security measures that could put their information at risk such as enabling their locations services and connecting to public WiFi.

These choices might mean that smartphone users are less aware of these media of data loss or have never experienced data loss through these means. This gap can be bridged by training, as suggested by some of the participants through verbatim feedback:
"Mobile security awareness is key as most users need to know how to protect their devices"
"Kindly let us know what the best practices for our phone safety are".

User Awareness on Security Risks
Figure 2 shows that a high number of users are aware that:

- Applications updates improve phone security.
- Some links shared or QR codes are not legitimate.
- Applications may contain spyware that can access private information on smartphones.
- Some banking applications pose as legitimate but instead steal banking information.
- Smartphone sensitive data can be transferred to a new user.
- Smartphones connected to open public WiFi hotspots expose personal and financial data.

These findings demonstrate that the awareness level of cyber security risk is high as most users are aware of common security risks. Users are generally aware of the most potential threats to their phones. Hence, there is a behavioural change gap between what users know and how they behave. For example, in Figure 2, 81% of users are aware that phone updates improve phone security. But as shown in Figure 1, only 46% of users update their smartphone. Likewise, in Figure 2, 86% of users are aware that open WiFi is risky yet 71% still connect to it.

4.0 Discussion

The findings show that Kenyan mobile users are knowledgeable on user security and have great concerns about risks that they are exposed to. However, users still make poor behavioral choices related to the use of smartphones, hence, making them vulnerable to cyber security attacks. This gap between user awareness and behavior is similar to the finding on employee's security awareness that showed a difference in employees' knowledge and employee behavior (Workman et al., 2008). This contrast might be because the information security awareness model of an individual is based on three dimensions; namely, knowledge (what users know), attitude (what users think or feel) and behavior (what users do) (Kruger & Kearney, 2006). Therefore, an impactful information security awareness model is one that is able to build on what users already know and what they think in order to impact behavioral change.

The findings also demonstrate that users' knowledge of security risks alone is not enough to change user behavior. Security behaviour is also influenced by motivation, persuasion, and social norms apart from user knowledge in security (Bada et al., 2015). Thus, an ABC Model was designed in which employees' attitude towards information security awareness was considered as an issue that is logical and emotional (Saracco, 2008). The model addresses the ABC aspect as follows; "A" Emotional aspect of attitude, "B" Behavioural component, and "C" Cognitive of attitude. Therefore, it is evident that when designing models to increase user information security awareness, it is important to consider the difference between what the users know and how they behave. To address this need, this paper proposes the use of a digital storytelling model to increase cyber security awareness among smartphone users in Kenya.

Proposed Digital Storytelling Model for Information Security Awareness

To meet the second objective of this paper, this section uses the processes displayed in Table 2 to design a digital storytelling model. This model is a basis for creating digital media for information security awareness among Kenyan smartphone users. In following this process, the model addresses the four major phases cited as a process guide for DST designers: pre-production, production, post-production, and distribution (Hashiroh & Norshuhada, 2016).

Characters

The study findings reveal that the age group with the highest representation at 53 percent was between the age of 20 and 30. From the sample participants, 71 percent were either working or self-employed and lived in urban areas. Hence, by using a character with similar characteristics who is in their twenties, working and living in an urban area in Kenya, the audience is more likely to relate the experiences

portrayed to their personal experience with using a public WiFi. The seven elements of digital storytelling stresses the importance of personalizing a digital story to help the audience understand the context better (Center for Digital Storytelling, 2005).

Language

Kenya is pervasively multilingual both at the societal and individual levels, and an average person speaks at least three languages. However, language policy in the education system recognizes English as the main medium of instruction in the urban areas at all levels of education. English is not only dominant in literacy, but in most public media avenues as well (Muaka, 2011).

Given that 87% of our participants live in an urban setting, and with 96% of them possessing good knowledge in IT, English has been chosen as the language of instruction for the video.

Narration Style

The approach used second-person narration in which, the story centred on a self-check approach to help our audience contemplate to change their behaviour when using public Wi-Fi. The second-person personal pronoun "you" was used by a narrator to identify and directly address a character that represents our audience. The advantage of using a second person point of view is that the audience, when directly addressed, may feel more intimately involved with the characters and the action in the story (Mildorf, 2016).

Multimedia Elements: Software

Adobe Premiere Pro was used to edit the video. Adobe Premiere Pro is a timeline-based video editing software application developed by Adobe Systems and published as part of the Adobe Creative Cloud licensing program. Premiere Pro is a comprehensive video editing software application used for editing videos, commercials, film, television, and online video.

Soundtrack

In digital stories, the present and abstracts can be textual, visual, musical, or a combination of the three. Before the narrator starts speaking, the story will have the music set the tone of the narrative. This is music that may activate certain associations and feelings to public spaces that provide WiFi. Orientation is the section of the story that sets the scene in time or place and introduces the people involved in it. The music, together with the sound of the narrator's voice has an orientation function. Since the story will be told in the second person, the voice introduces the main character in it. In the complication, the voice of the storyteller will be given precedence to be clearly heard. However, as the story evolves, different musical and sound effects will be used in order to signal a change in action. Seeing as the purpose of instructional digital stories is to advise and support, the resolution should be positive and encouraging (Bernaerts, 2016). Consequently, the music that will go with the resolution will be joyful and lively, with a rising volume that contributes to the positive effect of the resolution.

Media

A combination of visuals, voice narration, and music was used to present a narrative that was overlaid by videos taken by a camera, graphic layouts presenting statistics and instructional material, and external media such as other videos (Robin, 2016). The voice narration was heard at the appropriate volume (without distortion). Reading of the script was expressive, appropriately paced, and practiced, with no repetition (Campbell, 2012).

Script Content: Information Security Issue

Poor behavioural choices regarding security measures among smartphone users increase their risk exposure. The findings indicated that public WiFi was practiced by 71% of participants, locational services enabled by 69% of participants, and 75% of participants were not using antivirus. There is a dire need to urgently

address these matters. The model proposed addresses WiFi awareness, given that WiFi is among the top three security threats affecting mobile phones globally (Kaspersky, 2020).
The WiFi use is growing at unprecedented rate as mobile users are becoming heavy data users and hence WiFi is a cheaper option to use (Lee et al., 2012). However, this model can be replicated to raise awareness with other raised issues affecting mobile users.

Story Design: Information Security Belief Model

Figure 3 shows a process that was proposed to design an awareness model to promote secure behavior among internet users within the financial sector (Davinson & Sillence, 2010). Table 3 shows how this model has been adapted for this research as an Information Security Belief Model. This process was used to design the digital video.

The first part of the video portrayed the chances of becoming a victim of a public WiFi attack with the aim of increasing susceptibility to the risks involved. Similarly, the second part showcased the consequences of using public WiFi so as to show its severity. The third part explored if smartphone users are concerned about the use of public WiFi. These first three metrics are aimed at increasing a user's concern for protecting their information and ultimately motivating them to behave securely when using public WiFi. To further promote safe practices and behavior, the smartphone user must perceive they can control the occurrence of information security risk, for instance, by switching off automatic connection to public WiFi. Further, the smartphone user must also decide if the perceived benefits outweigh the costs. For instance, they must realize that switching off automatic connection to public WiFi requires minimal effort and could potentially prevent access to their information without their consent. The smartphone user should then know when to carry out preventive measures so as to protect their information towards the perceived benefits

Figure 3

Hierarchy of Contributing Factors towards Secure Behavior (Davinson & Sillence, 2010)

Table 3

Adaption of Figure 3 to an Information Security Belief Model

Perceived Susceptibility	What are the chances of becoming a victim of a public WiFi attack?
Perceived severity	How serious are risks involved with public WiFi & their consequences?
Information Security Motivation	Are users concerned that public WiFi can affect their information stored in mobile phones?
Perceived control	Can users prevent attacks from public WiFi by behaving securely?
Cues to action	When should smartphone users conduct secure behavior?
Perceived costs	What are the costs involved in carrying out the secure behaviour?
Perceived benefits	What are the benefits of carrying out secure behaviour?

Storyboard

To implement the information security belief model in Table 3, a storyboard was designed as shown in Table 4. A storyboard is a textual or a pictorial overview of all of the elements to be included in the digital story. A storyboard is a valuable component in digital storytelling process since it allow is organization of the media in a blueprint fashion before the actual creation begins (Robin & Mcneill, 2012). For example, Table 4 portrays, using grayscale images, a coffee shop, an airport lounge and a hotel lobby; all being places where a smartphone user may become a victim of a public WiFi attack. Using pictures to represent scenes that will be in the video, the storyboard goes on to showcase the dangers inherent with public WiFi and consequences of using it, in order to show its severity.

5.0 Conclusion and Recommendations

The finding shows that Kenyan smartphone users are knowledgeable on security measures available to them. However, they still behave in a way that leaves them vulnerable to mobile security threats. Therefore, user awareness should not only provide information to users but also address behavioural gap, that is, what users are doing. The awareness should be targeted, actionable, doable and provide feedback. The DSM is proposed to increase awareness among users and also change their behaviour. The DSM model has been created by adopting frameworks that have worked in other contexts and by inculcating the results drawn from participants of this research. Further, the DSM model has been modelled to fulfill all properties recommended for an impactful digital story.

The model is a prelude to a digital storytelling information security awareness video, which was tested for effectiveness among Kenyan smartphone users. The recommendation is that DSM can be tested further with various security issues affecting mobile security, with different sample population. The future work of this research is to constantly check on user risk level and develop more videos tailored towards user awareness by varying elements such as languages, narration style and characters.

References

Alsaleh, M., Alomar, N., & Alarifi, A. (2017). Smartphone users: Understanding How Security Mechanisms are Perceived and New Persuasive Methods. *PLoS ONE*, *12*(3), 1–35. https://doi.org/10.1371/journal.pone.0173284

Arsenijevic, O., Trivan, D., & Milosevic, M. (2016). Storytelling as a Modern tool of Construction of Information Security Corporate Culture. *Ekonomika*, *62*(4), 105–114. https://doi.org/10.5937/ekonomika1604105a

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2015). Cyber Security Awareness Campaigns: Why do They Fail to Change Behaviour? https://ora.ox.ac.uk/objects/uuid:cfed4907-d32a-4450-b075-ad37477b10d8

Bernaerts, L. (2016). Voice and Sound in the Anti-Narrative Radio Play. In *Audionarratology*. De Gruyter. https://doi.org/10.1515/9783110472752-009

Campbell, T. A. (2012). Digital Storytelling in an Elementary Classroom: Going Beyond Entertainment. *Procedia - Social and Behavioral Sciences*, *69*, 385–393. https://doi.org/10.1016/j.sbspro.2012.11.424

Center for Digital Storytelling. (2005). *StoryCenter*. https://www.storycenter.org/

Clisbee, D., Beierwaltes, P., & Eggenberger, S. K. (2019). Reducing Digital Dtorytelling Implementation Barriers in Nursing Education Workshops. *Journal of Continuing Education in Nursing*, *50*(9), 411–416. https://doi.org/10.3928/00220124-20190814-07

Communications Authority of Kenya [CAK]. (2018). *Fourth Quarter Sector Statistics Report for the Financial Year 2017/2018 (April-June 2018)*. Communications Authority of Kenya. https://ca.go.ke/wp-content/uploads/2018/10/Quarter-Four-sector-statistics-report-for-the-Financial-Year-2017-18.pdf

Davinson, N., & Sillence, E. (2010). It Won't Happen to Me: Promoting Secure Behaviour Among Internet Users. *Computers in Human Behavior*, *26*(6). https://doi.org/10.1016/j.chb.2010.06.023

Hashiroh, H., & Norshuhada, S. (2016). A Digital Storytelling Process Guide for Designers. *Journal of Telecommunication, Electronic and Computer Engineering*, *8*(8), 13–17. https://doi.org/http://journal.utem.edu.my/index.php/jtec/article/view/1312

Jumia. (2019). *Kenya Mobile Report 2019*. https://www.jumia.co.ke/sp-mobile-report/

Kaspersky. (n.d.). *Security Dangers of Public Wi-Fi - YouTube*. Retrieved August 13, 2020, from https://www.youtube.com/watch?v=XcghUy-8VRA

Kaspersky. (2020). *Top 7 Mobile Security Threats in 2020*. Kaspersky. https://www.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store?campaign=tcid_admitad_6ab325772c71d0e99b5c5a2683dc3a2e_240682_x4&ADDITIONAL_reseller=tcid_adm

Khalid, F., & El-Maliki, T. (2020). Teachers experiences in the development of digital storytelling for cyber risk awareness. *International Journal of Advanced Computer Science and Applications*, *11*(2), 186–191. https://doi.org/10.14569/ijacsa.2020.0110225

Kiboi, N. (2015). *Cyber Security as an Emerging Threat to Kenya Security*. [Doctoral dissertation, University of Pretoria]. https://repository.up.ac.za/handle/2263/50644

Kruger, H. A., & Kearney, W. D. (2006). A Prototype for Assessing Information Security Awareness. *Computers and Security*, *25*(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008

Lee, K., Lee, J., Yi, Y., Rhee, I., & Chong, S. (2012). Mobile Data Offloading: How Much Can WiFi Deliver? *IEEE/ACM Transactions on Networking*, *21*(2), 536-550. https://doi.org/10.1109/TNET.2012.2218122

Mildorf, J. (2016). Reconsidering Second-Person Narration and Involvement. *Language and Literature*, *25*(2), 145–158. https://doi.org/10.1177/0963947016638985

Muaka, L. (2011). Language Perceptions and Identity among Kenyan Speakers. In E. G. Bokamba (Eds.) *Selected Proceedings of the 40th Annual Conference on African Linguistics*, (pp.217–230). Somerville, MA: Cascadilla Proceedings Project. https://doi.org/Somerville, MA: Cascadilla Proceedings Project. www.lingref.com, document #2577.

Okuku, A., Renaud, K., & Valeriano, B. (2015). Cybers Security Strategy's Role in Raising Kenyan Awareness of Mobile Security Threats. *Okuku, Renaud & Valeriano*, *32*, 1–20. https://doi.org/http://dx.doi.org/10.11610/isij.3207

Quarshie, H., & Odoom, A. M.-. (2012). Fighting Cybercrime in Africa. *Computer Science and Engineering*, *2*(6), 98–100. https://doi.org/10.5923/j.computer.20120206.03

Rader, E., Wash, R., & Brooks, B. (2012). *Stories as informal lessons about security.* In Proceedings of the Eighth Symposium on Usable Privacy and Security, 1–17. https://doi.org/10.1145/2335356.2335364

Robin, B. (2016). The power of Digital Storytelling to Support eaching and Learning. *Digital Education Review*, *30*(30), 17–29. https://doi.org/10.1344/der.2016.30.17-29

Robin, B. (2008). Digital Storytelling: A Powerful Technology Tool for the 21st Century Classroom. *Theory into Practice*, *47*(3), 220–228. https://doi.org/10.1080/00405840802153916

Robin, B. (2011). *The Educational Uses of Digital Storytelling*. http://digitalstorytelling.coe.uh.edu/articles/Educ-Uses-DS.pdf

Safaricom PLC. (2018). *#Jitambulishe leo on 456. - YouTube*. https://www.youtube.com/watch?v=CDM1_yaKHNs

Saracco, D. (2008). Why and How Assessment of Organization Culture Shapes Security Strategies. In H, F. Tipton, & M, Krause *Information Security Management Handbook*,Vol.2 (6th ed., pp. 109–133). https://doi.org/10.1201/9781420067101

Serianu. (2017). *Demystifying Africa' s Cyber Security Poverty Line.* Annual Cybersecurity Report. https://serianu.com/downloads/AfricaCyberSecurityReport2017.pdf

Serianu. (2018). *Cyber Security Skills Gap*. Africa Cyber Security Report - Kenya. https://serianu.com/downloads/KenyaCyberSecurityReport2018.pdf

Skinner, T., Taylor, J., Dale, J., & McAlaney, D. J. (2018,4-7 April). *The Development of Intervention E-Learning Materials and Implementation Techniques for Cyber-Security Behaviour Change.* Convention of the Study of Artificial Intelligence and Simulation of Behaviour (AISB), Liverpool, UK.

Symantec Corporation. (2015). Internet Security Threat Report 2015. *Internet Security Threat Report*. https://doi.org/10.1007/s10207-014-0262-9

Workman, M., Bommer, W. H., & Straub, D. (2008). Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test. *Computers in Human Behavior*, *24*(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005

Zhang-Kennedy, L., Baig, K., & Chiasson, S. (2017, July11-13). *Engaging Children About Online Privacy Through Storytelling in an Interactive Comic*. Proceedings of British HCI 2017 –Digital Make-Believe.Sunderland, UK.https://doi.org/10.14236/ewic/HCI2017.45