Cyber Safety Awareness for first time Wi-Fi users in urban communities

Suné von Solms and Hannelie Nel
Faculty of Engineering and the Built Environment
Department of Electrical Engineering Science
University of Johannesburg
Auckland Park, South Africa
svonsolms@uj.ac.za, hannelien@uj.ac.za

Abstract

Africa has a fast growing information technology market where the rapid growth of mobile internet is aided by a drop in the cost of mobile handsets and wireless technologies. Improved wireless internet connectivity has enabled the use of mobile applications in assisting community members in banking, business, farming and healthcare. The City of Johannesburg provides free Wi-Fi to its residents in an attempt to build the capabilities of its residents and to train them to utilize and benefit from the broadband connections in their community areas. The Digital Ambassadors Programme is an initiative that employs Digital Ambassadors to train entrepreneurial youth in digital, business and life skills. These ambassadors then train residents in to access online services including banking, email, Facebook and job-search tools. However, it is important to educate people on cyber safety when teaching people to use technology for the first time given that people are naturally trusting and unaware of the dangers of the Internet. This paper discusses the cyber safety training material developed for the Digital Ambassadors and why cyber safety training is critically important when introducing residents to the advantages of the Internet.

Keywords
Cyber safety, Education, Digital activation

1. Introduction

The City of Johannesburg (CoJ) launched their Smart City project in 2015, aiming to roll out 1000 Wi-Fi hotspots across the city in 2015 and 2016 in order to provide free broadband connectivity to its citizens (City of Johannesburg, 2016; eNCA, 2016). Working towards their vision as a "world-class African City", the CoJ aims to accelerate Johannesburg's digital economy through digital inclusion, providing access to information and empowering citizens to interact with the City relating to services and service delivery (eNCA, 2016). The CoJ states that these facilities will enable students, employees, entrepreneurs, small, medium and micro-enterprises (SMMEs) and visitors to conduct their business on-the-go. This includes reading emails, updating social networks, conducting online banking or shopping; and online research.

In a partnership between the CoJ and the University of Johannesburg (UJ), the Digital Ambassador Programme (DAP) was launched with the objective to train approximately three thousand entrepreneurial youth as Jozi Digital Ambassadors (JDAs) in information and computer technology (ICT); and digital, business and life skills. These JDAs will work in their communities to introduce the residents of CoJ to the use and access of free Wi-Fi in their community areas (Pule, 2016).

The digital activation of the CoJ residents has the potential to empower the citizens of Johannesburg on new methods of learning, conducting business, job hunting and networking. However, in introducing the residents to the Internet and the advantages thereof, responsibility must be taken to introduce them to cyber safety as well. First-time users of technology can be naturally trusting and subsequently unaware of the dangers that the Internet may pose. It is therefore imperative to consider both the advantages and risks of freely-provided Internet access.

The objective of this paper is to demonstrate why it is essential that first time users of free WiFi are educated about the associated risks of the Internet whilst being active users; and to introduce the subsequent training material developed for the Jozi Digital Ambassadors. In support of the above proposition, the paper presents survey results of a study that was conducted on the preparedness of the Jozi Digital Ambassadors on cyber safety when they entered the programme. The paper is structured as follows: the mobile use landscape in the CoJ will be discussed in Section 2. The section that follows will provide an overview of the process, advantages and challenges of digital activation and Section 4 provides an overview of the Jozi Digital Ambassadors Programme and Section 5 an overview on the Internet usage profile of the Jozi Digital Ambassadors. Section 6 mentions educational resources and the advantages thereof; and Section 7 discusses the preparedness of the JDAs when entering the field. Section 8 concludes the paper and suggests the way forward.

2. Urban Mobile Usage Landscape in CoJ

Access to mobile services continues to grow exponentially in South Africa (SA), with individual mobile phone ownership estimated at approximately 86% of the adult population for people 15 years or older. Approximately 70% of adult users in urban South Africa access the internet via a mobile phone. Unfortunately, the cost of communication services in South Africa remains high compared to African and global standards (Gillwald, 2012). The cheapest mobile prepaid product in South Africa costs approximately seven and a half times more than a comparative product in Africa (Gillwald, 2012). The price in airtime (for voice communication) has dropped significantly, but proves to have little impact as South Africa has seen a rapid decline in the use of voice services, as the use of data and services which requires data are on the increase.

In addition to the high cost limiting Internet use, a vast majority of previously digitally disadvantaged SA citizens are not aware of what the Internet is or what services are offered. According to a study by ResearchICTAfrica (2012), reasons to why citizens in urban areas do not use the Internet include the following:

- Not knowing what the Internet is;
- No Internet connection availability;
- Citizens do not know how to use the Internet; and
- The Internet is too expensive.

The CoJ has approximately 4.8 million residents, where only fifty percent of those have regular access to the Internet. According to the previous major of the City of Johannesburg, digital access is “becoming as much an equity issue in our society as access to water and electricity” (Raborife, 2015, pp 1). Considering these statistics, it is clear why cities are starting to roll out free WiFi to its citizens in an effort to accelerate digital inclusion by empowering their citizens to improve access to information and services.

3. Advantages and Challenges of Digital Activation

3.1 Advantages of mobile usage

The use of mobile applications is proving to greatly improve the welfare and lifestyle of Africans, as access to the Internet through mobile phones in Africa is becoming more widely available (PWC, 2012). M-Pesa, the Kenyan money transfer service by Safaricom, is an excellent example of how banking services are accessed and utilised by users through their mobile phones. M-Pesa had reported over 900 million users in 2015 and 42% of Kenya’s gross domestic product is transacted on M-Pesa (Migrant, 2013). In South Africa, mobile banking applications are offered by most of the larger banks. The mobile banking applications enable the user to transfer money, make payments, check balances and access other banking services. Mobile banking through cell phones and mobile applications are rapidly growing in South Africa, where mobile banking transactions are growing at approximately fifty percent per annum in terms of volume of transactions. It is also predicted that in the next three to five years the majority of banking transactions will be performed on mobile devices (SBGroup, 2016).

Social media and electronic communication applications, such as email and WhatsApp, are also having a significant impact on the rural African landscape. The SA Social Media Landscape 2014 revealed that the WhatsApp instant messaging (IM) application is used by at least 10.6 million South African adults on their phones (PWC, 2012).

3.2 Challenges of mobile usage

In using mobile applications, users must be aware that the applications on their mobile device may require and use information of the user. This may include the following (SBGroup, 2016):

- Phone and email contacts
- Call logs
- Internet data
- Calendar data
- Data about the device's location and unique identification numbers
- Information about the application is used

When installing these applications, the users must provide permission for the applications to access the information, but often this function is overlooked. In addition to sharing information about the users and their user patterns, the utilization of applications can also lead to a range of security concerns. Applications must be updated regularly to insure that all security features are up to date. When downloading infected applications, mobile devices may become infected with malware, which can provide hackers access to the user's personal information and applications.

However, one of the biggest challenges associated with the use of mobile devices relates to the general use of these applications. Users must understand that any information sent over the internet cannot be controlled. When a user uploads or shares content online, he/she must be aware that, even if it is only shared with a friend, the content can easily be spread further without the consent of the original sender. In addition, the user may be exposed to various attempts of social engineering, whereby criminals obtain private information and potentially inappropriate content.

4. Overview of the Digital Ambassadors Programme

The local municipality of the City of Johannesburg, as part of its developmental service delivery model, is focusing on building the capabilities of its residents to enable them to provide services to meet the city's resources needs (PWC, 2012). As part of the roll-out of one thousand WiFi hotspot throughout Johannesburg, CoJ will be capacitating approximately three thousand Jozi Digital Ambassadors to train its residents to utilize and benefit from the broadband connections in their communities. These ambassadors are mentored by university students and trained in digital, business and life skills. They are provided with electronic tablets, branded clothing and marketing material to reach a targeted seven hundred and twenty thousand CoJ residents over an eighteen month period. Residents will be trained to access online services, including banking and digital map navigation; as well as interact with the Maru a Jozi (cloud) portal to link up with a range of online services including work and job-search tools.

The JDAs attend a range of training sessions, covering various topics such as business basics, how to work with people and relevant digital technology. In addition to the training sessions, the JDAs can do additional online training which includes videos, journals and information sessions with assigned university student mentors.

5. Digital Profiles of Ambassadors

A subset of the JDAs who attended the formal training event of the Digital Ambassadors Programme was presented with a survey on general cyber security and their use of the Internet. Its objective was to ascertain the general use of the Internet by the JDAs; as well as their basic knowledge of cyber security related issues and risks. In total 316 JDAs completed the survey. The results of the survey are discussed in the subsequent sections.

5.1 Internet usage profile

According to survey results, 73% of the JDAs stated that they access the Internet several times a day, primarily from their homes (57%), but also when in public places, such as libraries or internet cafes (60%). Approximately 74% of the JDAs utilize their mobile phone to access the Internet, whereas 18% use a tablet. The various devices used by the JDAs to access the Internet are shown in Figure 1. Note that JDAs could select more than one option, thus the sum of the percentages will be greater than 100%.

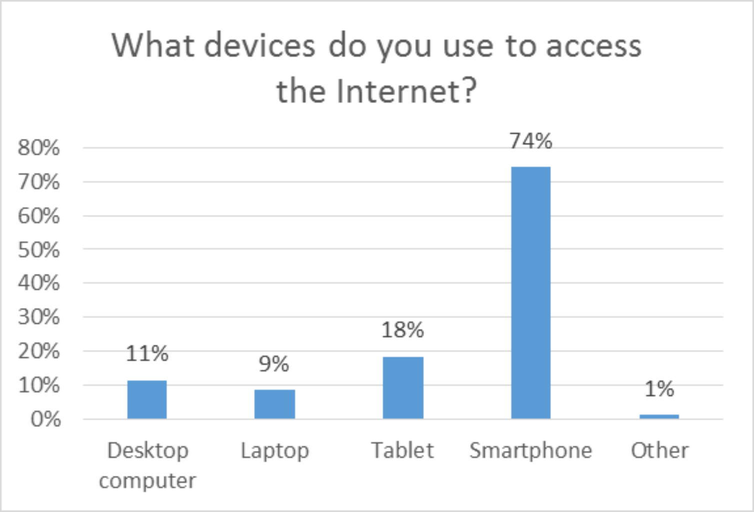

Figure 1. Internet access through various devices

When asked what activities the JDAs engage in online, the following feedback was received: the majority of JDAs engage in social networking (59%) and email (54%). Only 24% utilize online banking and only 17% of the JDAs buy or sell goods online. The results are shows in Figure 2.

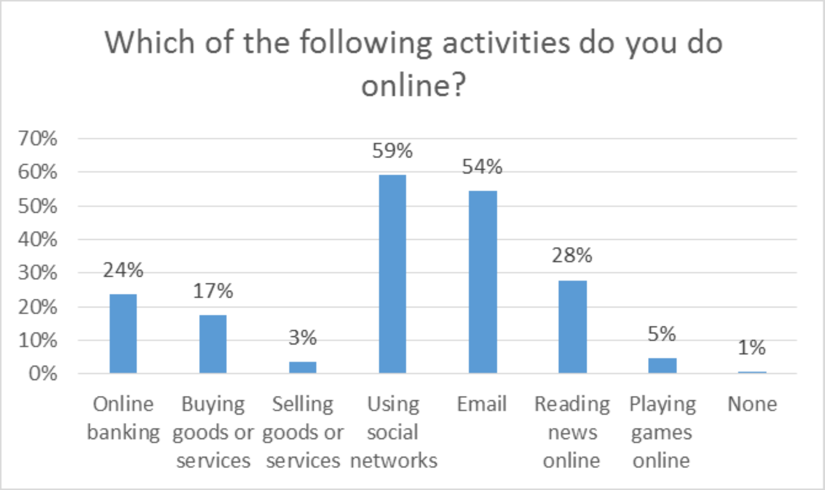

Figure 2. Access to online activities

When responding to the question "How confident are you about your ability to use the Internet for things like online banking or buying things online?" a total of 39% stated that they are very confident and 36% stated that they are fairly confident. However, 34% of the correspondents stated that they are concerned about the security of online payments whilst 29% responded that they prefer to conduct a transaction in person.

5.2 General cyber safety knowledge

The survey indicates that most of the JDAs have heard about cybercrime and other cyber safety related issues via the Internet (29%) or from other people (24%). A total of 15% stated that they had not heard anything related to cyber security related issues in the previous twelve months and a total of 26% of JDAs stated that they do not feel informed about the risks of cybercrime. Asked how their concerns about cyber security risks change the way in which they use the Internet, the result indicate that it does not influence their behaviour dramatically, as indicated in Figure 3. Although 37% of the respondents state that they are likely to share less personal information online, small percentages of the respondents indicated that they use anti-virus, only use their own device or use different passwords for different sites.

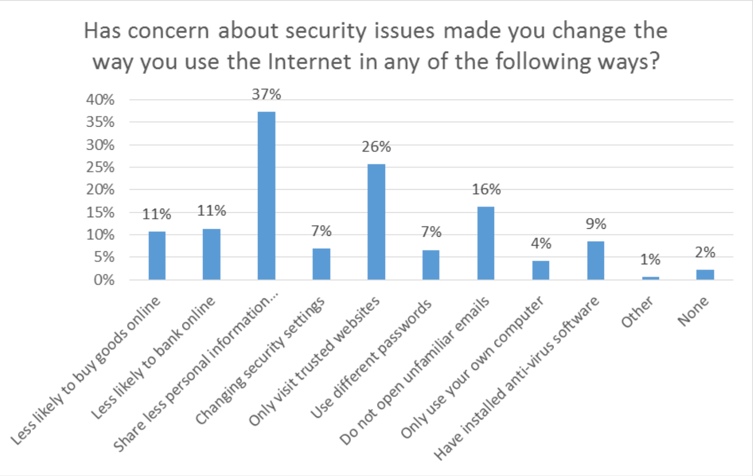

Figure 3. Change in Internet use due to risk concerns

Based on the results of the survey it can be deduced that, although the JDAs state that they are aware of cyber safety risks, they may not realize the impact of it or know how to reduce the potential risks. The inclusion of cyber safety training material in their training programme was therefore imperative to improve their awareness on the topic so that they can inform and train the CoJ residents as well.

6. Cyber Safety Training Material

This section provides a short overview of the information contained in the training material on cyber safety provided to the JDAs. The main sections focused on in the training includes:

- WhatsApp
- Email
- Facebook and social media
- Cell phone banking and shopping

These topics cover the most popular aspects which the JDAs need to take into account when training the residents.

Firstly, it is imperative to state in training that an Internet user can't control what happens to anything that is sent over the Internet, including sending emails, WhatsApp messages or posting on Facebook. An Internet user must accept that anything that is send over the Internet is public knowledge and once it is sent, it can never truly be deleted. In addition, it must be understood that nobody else must be trusted with the safety of personal information. It is the user's own responsibility to keep it safe, therefore private information must not be shared with anybody, including people that may seem trustworthy.

The subsequent sections provide the basic information provided in the training material.

6.1 Email

One of the first activities which the JDAs can teach a resident, is to open and use an email account. JDAs assist the resident to open a Gmail account and how to send and receive email messages. As email has become one of the simplest forms of communication for business and private use, an email address enables a user to instantly send a message to anybody around the world. By understanding the convenience of e-communication, the user must also be taught that, as a result, cyber criminals can also utilize emails for fraudulent and illegal activities. Cyber criminals can send emails to residents where they pretend that they are somebody that an email account holder may know or trust. Criminals can also appeal to the goodwill or nativity of the user to obtain personal or sensitive information from them. The following simple tips on safe email use are included in the training which will supplement the training on how to create an email address and how to use it:

- Unknown sources: When an email is received from an unknown sender, the user should not respond to that mail. The account holder should never respond to an unknown sender by sending any personal information, no matter the cause or appeal.
- Malicious Attachments & Links: The user must only click on links or open attachments in emails if they are expected and the sender is known. Criminals can send emails that look like they come from a bank or trusted organization in order to gain the trust of the account holder and trick them. These links and attachments may be infected with malware that can harm devices or steal personal information.
- Obtaining personal information: Users must be aware that they must never share sensitive information over an email, for example, banking details or passwords. Banks will never ask their customers to email banking details or password to them.
- Scams: If a user receives an email that looks odd or sounds too good to be true, it probably is. A user must never respond to an email claiming that they have won a prize. These emails must be deleted, as they are scams.
- Passwords: The email account user must never share email password with anybody, even family or friends. Password should be changed regularly.
- Privacy: The email account holder must avoid giving out their email address publicly without a good reason.

6.2 WhatsApp

Another popular application introduced to the residents is WhatsApp. The fact that messages can be sent and received through the use of the free Wi-Fi appeals to the residents, as they had to previously pay to send traditional text messages. WhatsApp is one of the most popular instant messaging platforms in the world which makes chatting to friend and family extremely easy and convenient. However, cyber criminals use WhatsApp too, so any WhatsApp user must be aware of possible risks so not become a victim of a cyber-attack through WhatsApp. The following tips for safe WhatsApp use included in the training material:

- Unknown chats: The WhatsApp user must chat only to people who they know. Criminals will attempt to become a user's online "friend" in order to gain their trust. Users must never respond to an unknown person by sending any personal information.
- Sending personal information: A WhatsApp user must never send any personal information (banking details, passwords, and addresses), sensitive information or inappropriate/sensitive photos over WhatsApp.
- Inappropriate content: If a user receives a message/video/photo that makes them feel uncomfortable, the user must block the sender's number and not respond to the message.
- Scams: If a user receives a WhatsApp message stating that they have won a prize or that they can claim money, the user should be blocked and the message deleted. Users must recognise these messages as scams and not respond.
- Privacy: Any WhatsApp user must avoid giving out their phone number publicly without a good reason.

6.3 Facebook

Many residents ask the JDAs to assist them with Facebook. Facebook is the number one social media platform in the world and the training material must inform the users that cyber criminals are also active on Facebook, searching for targets to provide them with personal information and access into their lives. The following simple tips are included in the training material on how to keep Facebook accounts and private lives safe:

- Real friends: All Facebook users must only invite/accept friends that they know in real life. Criminals will attempt to become online "friends" with innocent Facebook users in order to gain their trust. Users should never respond to an unknown person by sending any personal information or befriending them.

- Privacy settings: Facebook makes everything public, unless privacy options are changed to do otherwise. Users must make sure that only their friends can see their Facebook profiles. Users are reminded that they do not tell strangers in the street about your personal life, so they should not do it on Facebook.
- Private information: A responsible Facebook user should never post any private or sensitive information on Facebook, including cell phone numbers, address, banking details. Users must never post updates such as "I am home alone", constantly update your location or post photos that they will later regret posting. A user must remember that information on Facebook is not private, even if it is only send it to friends.
- Passwords: Facebook users must not share Facebook passwords with anybody, even family or friends. Change your password regularly – make it easy to remember, but heard to guess.
- Inappropriate content: If a user receives a message/video/photo that makes them feel uncomfortable, that person should be blocked and no response given.

6.4 Cell phone Banking

Another skill offered by the JDAs is to teach the residents how to use cell phone banking. Cell phone banking is very convenient as it provides an alternative to standing in long queues at the bank or ATM. As cell phone banking requires extremely sensitive information, it is imperative to know that cyber criminals will work very hard to try and obtain a user's banking details and password. In order to keep money safe, the cell phone banker must know the following instructions:

- Protect private information: A Cell phone banker must never provide any banking details to anybody, including family or friends. The bank will never ask a customer to send them account information or password via SMS, email or phone call.
- Security: When conducting cell phone or online banking, a user must never use anybody else's computer, phone or tablet (including friends and family) to conduct banking. The user has no control over the device and cannot know of their device is secure.
- Wi-Fi Security: Unencrypted Wi-Fi spots should never be used to conduct banking. When Wi-Fi do not require a password, assume the user must assume that it is unsecure and that anybody can see personal banking information.
- Passwords: The user must never share banking password with anybody, even family or friends. Banking passwords must be changed regularly.
- Sign out: User must be reminded that they must always sign out of the banking application after completing transactions. Phones must be locked and protected with a password.

7. Cyber Safety Preparedness

After the conclusion of the cyber safety training, a second survey was presented to 260 JDAs. This survey tested the JDAs on their practical cyber safety preparedness. The survey was divided into 5 sections, asking questions relating to the use of WhatsApp, email, social media, cell phone banking and online shopping as well as general cyber safety aspects. The questions included in the survey were all practical questions, setting a scenario and asking the JDAs how they will respond. For example: You are visiting a website that a friend told you about. The site requ ests your name and phone number so you can enter a contest. What should you do?

7.1 Findings

Approximately 75% of the JDAs stated that they will not share their personal pictures with a person that they have never met, but when asked what to do when a stranger wants to chat over WhatsApp, approximately 45% indicated that they will accept the friend request. About 40% of respondents stated that they will not click on links they receive via WhatsApp, but approximately 45% stated that they will click on a link if it were sent by their best friend whom they trust. The majority of respondents (93%) stated that they will not react to cyber bullying via WhatsApp, whilst 82% indicated that they will not respond to the messages and block the sender.

The JDAs were asked what they will do if they receive an email claiming the sale of smartphones at a good deal with an included attachment (pdf or picture). 45% of the respondents stated that they will not open the email and delete it, but 52% stated that they will open the attachment as a pdf or picture. Asking the JDAs how they would respond when receiving an email claiming that they have won a prize, the majority of respondents (82%) stated that they will not respond to the mail, whilst 16% will first try to find out more before responding.

The JDAs were asked how they would respond if a new Facebook friend, whom they do not know in real life, asked for personal information, like an address and phone number, or to set up a meeting. Approximately 40% indicated that they will never share this information online, whilst 32% indicated that they will never agree to meet a stranger. Approximately 73% of the respondents also indicated that they will not use online social platforms to look for new friends; however, a total of 55% of JDAs stated that they are comfortable accepting friend requests from people whom they do not know personally, but have friends in common with. 23% of the respondents stated that any personal information is safe to share on Facebook as long as only their friends can see it.

Results indicated that the JDAs are more cautious when it comes to cell phone banking and online shopping compared to social media. 56% of JDAs indicated that they will not respond to an email claiming to be from the bank requesting banking details whereas a further 43% indicated that they will first confirm with the bank before possibly responding to the email. Approximately 72% indicated that their online banking profile has a unique password and 69% stated that they will never share their password with anybody else. However, the remaining respondents (approximately 20%) stated that they will share their banking passwords in certain circumstances, like when asked for it by a banker or a friend. 90% of the respondents stated that they would only use their credit card for online purchases if the website is trustable, which includes a secure https connection, a locked padlock icon and a dependable reputation.

When asked when it is appropriate to utilize free, public WiFi, approximately 91% of the JDAs indicated that it should only be used for browsing, information gathering and social network usage; but for no activities requiring sensitive information. Only 5% of the JDAs indicated that their phones are set to automatically connect to free WiFi. Alarmingly, 80% of the JDAs stated that they will take a lost flash drive found in a public place to either use it, format it to use in future or plug into their computer to try and find the owner. Only 20% stated that they will leave it alone. When asking the respondents what personal information is safe to share online, the following results were obtained:

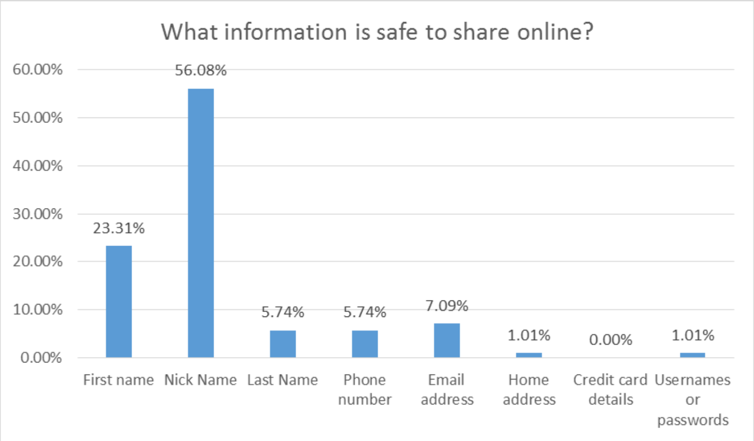

Figure 4. Name of the figure

It can be seen from the graph that all of the respondents indicated that they will not share their credit card information and only 1% stated that they will share their username and password.

7.2 Discussion

When considering the results of the second survey after the cyber safety training was completed, it can be seen that the JDAs possess a general framework for cyber safety security. The majority state that they will not share sensitive information online, that they do not share their passwords, that they do not actively seek to make friends online and that they will not share pictures with people they have not personally met.

In contrast, however, when setting a scene where friends, family or other trusted people are involved, the JDAs seem to be more trusting and will act differently that initially stated. Nearly half of the respondents stated that they will click on a link if they know it was sent by their best friend, as their best friend will only send safe links. Approximately 73% of the JDAs stated that they do not actively search for friends online, but more than half are comfortable befriending people they do not know online. Furthermore, approximately 23% of the JDAs continue to say that they are comfortable sharing personal information online if it can only be viewed by their friends, not considering that some of those "friends" they have never met before. 1% of the JDAs stated that usernames and passwords are not safe to share. However, in a scenario-based question, up to 30% of the JDAs stated that they will share their banking username and password when a person they consider trustworthy requests it.

From the survey results, it is clear that although the JDAs have a broad understanding of cyber safety risks, they are extremely trusting. Their trusting natures may expose them to risk when working on the Internet with the various technologies and platforms.

8. Conclusion

The Jozi Digital Ambassador project was launched in the City of Johannesburg to train up to 3000 entrepreneurial youth as Jozi Digital Ambassadors. The aim of the Ambassadors is to work in their communities to introduce the residents of the city to access and use the free WiFi in their communities. As the city aims to introduce their residents to the advantages of the Internet, it is also incumbent on them to make the residents aware of the associated risks of online activity.

This paper an overview of the training content on cyber safety which is the starting point for the Digital Ambassadors Programme to address cyber safety awareness for first time WiFi users in urban communities. A survey was presented to the JDAs to determine if the training material is sufficient for them to responsibly train the city's residents of the possible risks of the digital world. The results of the research show that the trained ambassadors are aware of cyber safety risks, but are still very trusting. Their trusting nature may lead to important cyber safety information not being taught to the residents, which might expose the residents to various cyber risks. Future work can include the expansion of the training material to ensure that all JDAs understand that cyber safety aspects apply not only to strangers, but to family and friends as well.

In training residents to use email, social media as well as internet banking, the residents must be educated on the safety aspects related to these technologies. There lies a great responsibility in educating people on cyber safety issues when teaching people to use technology for the first time as people can be naturally trusting and unaware of the dangers that the Internet offers. Therefore it is essential for the Digital Ambassadors Programme to not only to focus on the advantages of free Internet usage, but to train the CoJ residents on how to use it safely as well.

References

A. Gillwald, M. Moyo and C. Stork, Understanding what is happening in ICT in South Africa, *Research ICT Africa*, 2012.

A. Pule, Free Wi-Fi to keep city residents connected, Available: http://www.vukuzenzele.gov.za/free-wi-fi-keep-city-residents-connected, Accessed April 2016.

City of Johannesburg, Residents to join Joburg's digital revolution, Available: http://joburg.org.za/index.php?option=com_content&view=article&id=9916:residents-to-join-joburgs-digital-revolution&catid=88:news-update&Itemid=266, Accessed April 2016.

eNCA, Braamfontein officially free wi-fi zone, Available: https://www.enca.com/south-africa/joburg%E2%80%99s-braamfontein-officially-free-wifi-zone, Accessed April 2016.

Internet Research, WhatsApp takes SA by storm, *worldwideworx*. Available: http://www.worldwideworx.com/whatsapp/, Accessed March 2016.

M. Raborife, City of Johannesburg to help unemployed youth, Available: http://mg.co.za/article/2015-05-06-city-of-johannesburg-to-help-unemployed-youth, Accessed April 2016.

Migrant, M-PESA International Money Transfer Service, *Safaricom*, Available: http://www.ilo.org/dyn/migpractice/migmain.showPractice? p_lang=en\&p_practice_id=70, 2013, Accessed November 2013.

PWC, Telecoms in Africa: innovating and inspiring, *Communications Review*, 2012.

SBGroup, Future of banking in Africa is mobile, *Standard Bank*, Available: http://community.standardbank.co.za/t5/Blog/Future-of-banking-in-Africa-is-mobile/ba-p/921, Accessed May 2016.

Biography

Suné von Solms is a Lecturer at the Faculty of Engineering and the Built Environment (FEBE) at the University of Johannesburg. She obtained her M.Eng and Ph.D. in Computer Engineering at the North-West University in the field of telecommunication and error correction coding. She is registered as a Professional Engineer with ECSA and is a member of the IEEE and SASEE. She is involved with the FEBE Research and Projects office, where she conducts research into the social and human aspects of engineering, including engineering education and the impact of technology in society. She is the author of over 25 conference papers, journal papers, workshop papers and book chapters, has served on 5 conference and workshop programme committees and is a referee for roughly 10 local and international conferences and journals.

Hannelie Nel is a Senior Research Associate at the Faculty of Engineering and the Built Environment, University of Johannesburg and a Visiting Associate Professor at North-West University, South Africa. She holds a Doctorate in Engineering Management with twenty years' experience in both industry and academia. Dr Nel is a Fellow of the Southern African Society for Industrial Engineering and currently serves on the Boards of the Society for Engineering Education; and the TechnoLab and Metal Casting Technology Station of the University of Johannesburg. She is an Associate Member of the Institute of Directors in South Africa; and a Member of the International Women's Association.