IJST EXPLORE International Journal of Science and Technology
CENTRE OF PROFESSIONAL RESEARCH PUBLICATIONS
ISSN 2049-7318
International Journal of Science and Technology Volume 4 No. 12, December, 2015

Security and Usability Enhancing E-Service Marginalization for Digital Vulnerable Groups

[1]Muchiri Michael Njoki, [2]Franklin Wabwoba, [3]Elyjoy Muthoni Micheni
[1]Department of Information Technology, Kibabii University;
[1]Department of Information Technology, Dedan Kimathi University of Science and Technology, Kenya
[2]Department of Information Technology, Kibabii University, Kenya
[3]Department of Management Science and Technology, the Technical University of Kenya, Kenya

ABSTRACT

In the new information society, services are delivered electronically making it cost effective, efficient and convenient for both the government and private firms making ICT a major facilitator of social economic development. However, a new form of exclusion is emerging in the provision of e-services due to security usability. This paper has discussed the e-services concept and its contribution to digital exclusion. It explores security, usability, and the contribution of security usability to digital exclusion of vulnerable groups hence social exclusion. Just like security, usability is a critical aspect in adoption of e-services. Security alone without usability is not sufficient to building trust among users of online services. Where there is lack trust arising from inadequate security just like where a system is not usable amongst users, many a time will lead to it's not being used the system. Those who abandon the use get excluded. The paper is a product of an ongoing study on security usability to achieve inclusivity.

Key Words: *Digital Exclusion; Digital Vulnerable Groups; E-Service Marginalization; Information Society; Security Practices; Usability Practices*

1. INTRODUCTION

The emerging of ICT and related technologies has without doubt had a great influence in the modern society (Smith et al., 2011; Hellman, 2008). Among the influences, the technology has for instance altered some of the cultural norms. A new information society has emerged in which ICT has been identified as a major facilitator of social economic activities. This society lives in a virtual world that is only accessible digitally and, according to Grahams (2011), is full of opportunities and capabilities. Among the differences made by ICT is the nature, the structure and the packaging of service delivery. Delivering services electronically, often referred to as e-services, is cost effective for both the government (Alsmadi, 2011) and private firms (Visser, 2013) as it is convenient for the consumer (Chavan, 2013). For Private firms, e-services provision provides a wider market reach for them to reduce the cost of production and offer a competitive advantage among other benefits (Mitrovic et al, 2013).

Within the Governments, ICT has simplified service delivery making the services more affordable for citizens and in the process has made crucial contributions toward an enabling environment for social growth (Singh & Chauhan, 2014). Governments across the world are thus adopting e-governance in an effort to improve their services and relationships with citizens (Alshehri et al., 2012). The Kenyan Government is one such government. In Kenya, citizens can search and register company names through their mobile phones. Financial services are now available twenty four hours, seven days a week, thanks to e and m-banking facilities. Among the great innovations in the country include the Huduma centers that offer digital outlets to most of government services and the MPESA system of mobile money transfer. Development agencies across the world are also increasingly advocating for adoption of ICT to spur growth and sustainable development (UN, 2012).

The information Society is however not without challenges. In the provision of e-services, a new form of exclusion, digital exclusion, has emerged. An exclusion suffered by those unable to benefit from the e-services. The irony of it all is that those already included are better placed to enjoy the benefits that the Technology bears. The poor, those living with disability, the uneducated and those in remote areas are more often limited on how much they can access and use ICT. This is likely to widen the social and economic gap between those who have and those who have not. This in itself undermines the efforts for building an equal and cohesive society.

As had been noted earlier, ICT is playing a major role in social economic development. Its adoption is critical in spurring growth and sustainable development (UN, 2012). Those unable to access its affordance therefore are disadvantaged and marginalized (Seale, 2009). The difference between those accessing and using ICT is often referred to as digital divide. From this perspective, ICT is viewed as a resource that is not within reach of the marginalized. The digitally excluded are said to be on the lacking side of this divide. They do not partake of the benefits that come with access and use of ICT (Mervyn, 2014). They are barred from experiencing and being part of the virtual world (Grahams, 2011). Indeed Grahams (2011), advocates a rethinking of the digital divide where the economic, cultural, political and technological positional ties of those attempting to access the technology and the barriers that obstruct use of e-services will be considered.

Accessing, using and benefiting from digital services can also be compromised by among others things, the security and usability features of the systems. Despite all the factors stated, one form of exclusion that cuts across is denial of service resulting from poor security usability. One of the most fundamental issues on e-services provision is security. Whether on ecommerce or when accessing government services online, there is exchange of sensitive data that should be protected. The design and implementation of the security aspect of the eservice may have an impact on the utilization of the service.

E-services move

An electronic service or e-service is a service offered through a digital platform (Cristea et al., 2012). This includes computer, internet, mobile phone and cloud computing based services. Any service that's offered or accessed online is an e-service (Visser, 2013). Most of the digital platforms such as grid systems and cloud systems are aimed at provision of e-services (Cristea et al. 2012). E-services come in all shapes and forms. They may include attending of classes online, conducting job interviews (Minichielo et al., 2013), seeking medication, buying and selling of commodities, filing tax returns, news delivery, financial and banking services (Chavan, 2013),,reserving flights and hotel services among thousands of other services that are being availed online today (Visser, 2013, Minichielo et al., 2013).

Both public and private organizations today prefer to offer their services electronically (Michalski et al., 2014). The increased use of e-services is promoted by the continued increase in capacity, mobility, accessibility and affordability (Mitrovic, 2013; Yihua Yang et al., 2013) of ICT. According to Mitrovic (2013) ICT has induced a digital dimension on every aspect of human life. This has led to a self-service society (Hellman, 2008). The self–service societies are also attributed to commercialization of services and the need to be cost effective (Hellman, 2008).

The benefits of e-services to the customers and citizens is convenience (Alsmadi, 2011) in that they are able to access services at a time and place most appropriate to them (Hellman, 2008), and affordability due to the reduced cost of production for the providers. According to Cristea et al (2012) e-services "…are easy to use, can dynamically discover each other by using the publish-subscribe-notify mechanisms, and can communicate in timely and consistent information…"

Governments across the globe have largely moved digital in providing services to citizens (Alshehri et al., 2012) through e-governance. E-government services can be classified as Government to Government(G2G), Government to Business(G2B), Government to Employee (G2E) or Government to Citizen(G2C) (Carter & Belanger, 2005; Alshehri et al., 2012). ICT and e-governance has benefited citizens from an increased democratic space that empowers them (Rainie, 2011; Alshehri et al., 2012; Visser, 2013). ICT has become a tool to reform governance (Chauhan & Singh, 2014). Governments embracing ICT have become "more proactive, efficient, transparent and especially more service oriented towards its clients" (Chauhan & Singh, 2014) by the end of it, their services to the citizens are highly expanded in a cost effective manner (Chauhan & Singh, 2014).

Digital marginalization

ICT and related technologies have given rise to new capabilities to the human race. As Smith puts it "Mobile phones constitute the basis for one of the greatest expansions of human capabilities in known history, and in a remarkably short timeframe. Furthermore, this expansion is expected to continue apace and, more likely, to accelerate" (Smith et al., 2011) lack of access to this technology thus leads to a form of marginalization and exclusion. Digital marginalization has been discussed in many forums as the digital divide. An article posted on the business daily of the nation media on august 23rd 2011 quoted the then Kenya Information and Communications Permanent Secretary, Dr Bitange Ndemo, saying "while this phenomenal growth of the ICT sector is envisioned to serve as an engine for economic growth in the 21st century, it may also if not properly managed, create a disparity between those without and those with access to the ICT infrastructure and services", according to that article, the minister said this while launching an ICT access gap study that had indicated that "despite Kenya's rapid ICT growth there is danger that some section of the masses, especially in rural areas could be left behind".

Digital marginalization is being on the lacking side of digital divide. It is characterized by inability to benefit or participate in the information society (Charleson, 2012). Digital divide is the inequality in accessing ICTs and internet between individuals, households, enterprises and regions at different socio-economic levels (OECD, 2001 ; Graham ,2011; Bosch et al., 2010) It is also used to refer to the difference in access and use of the latest Information Technologies (EUC, 2014). The interest on the digital divide is generated by the effects that ICT has had in the society. The debate on social and economic effects that lack of, or limited use or access to ICT has cannot be considered lightly. Graham (2011) asserts that in the telegraph era long before electronic computers were invented, it was predicted "that communication technologies would bring about positive economic and social development in the global periphery" (Graham, 2011; Marvin, 1988). And those not having the technology would be disadvantaged as uneven flow of information and different levels of access to technology would exacerbate social and economic segregation (Graham, 2011). The idea has become a reality today. ICT and related technologies continually influence the modern society (Smith et al., 2011; Hellman, 2008). Those without ICT are greatly disadvantaged (Mitrovic et al., 2013; Visser, 2013). "Inability to access or use ICT has effectively become a barrier to social integration and personal development" (DG Information Society and Media Group, 2008; New Zealand Computer Society, 2010).

Digital exclusion is manifested in different levels; Access, use and benefits. Barriers to access include the cost of ICT facilities which may be inhibiting for the poor. Those from poor countries or remote areas may be locked out due to lack of ICT infrastructure. Other secondary resources like reliable

power supply may also be a barrier (Wyche & Murphy, 2013). Another access level challenge is the type and quality of technology available. The poor may not access the latest technology. The internet speeds in developing countries on average are very low. While many countries in Africa could be employing old PCs in schools for giving occasional computer studies to the pupils, schools in first world countries are having fully computerized classrooms complete with Virtual learning environments and integrating ICT in teaching and learning for different subjects. This translates to early skills acquisition and adoption. Lack of use may be a consequence of lack of access. Other barriers to use may include lack of skills or attitude and cultural related barriers. Lack of access and use further leads to denial of services, benefits and ultimately exclusion.

Even as the cost of those outside the networked society continues to be ignored (Cushman & McLean, 2008) and consequently excluded from the society. The already marginalized in other sectors are the worst affected (Hick, 2008). A high correlation between social and digital inclusion is evident from many other researchers (Mervyn, 2014; Tapia et al., 2011). Factors such as geographical location, race, economic status, gender, physical disability, literacy and age (Lor, 2003; Patil & Bansode, 2011) have been linked to digital exclusion. Those marginalized lack access, skills, knowledge, and abilities to use information on the Internet, and other information technologies and services. ICT as a resource has remained out of reach from the marginalized. This digital exclusion has also lead to other social divides including political, economic and cultural divide (Fuchs & Horak, 2006).

The role of digital divide in marginalization debate can be viewed from different perspectives (Grahams, 2011). One way is to view it as an obstacle to movement of people and places temporally along a pre-defined path of development. Those without are left out of development. The second view separates people and places into those unable to access and participate and those accessing and participating in the 'global marketplace,' and 'information revolution,' (Graham, 2011). The view portrays two worlds, the physical and the virtual. It places those with access as a part of a virtual world, full of opportunities and capabilities, that those without can never be part of. Either way, there is need to bring in those left out.

Development agencies across the world are increasingly advocating for adoption of ICT to spur growth and sustainable development (UN, 2012). According to the Information Policy and Access Center at the University of Maryland (IPAC), equal access to and participation in online environment is a necessity for education, employment, finance, and civic engagement owing to the ubiquitous nature of the Internet and accompanying services (IPAC, 2012). As such, the technology has been viewed as a remedy to the social economic problems (Alshehri et al, 2012; Animashaun, 2014) in both developing and developed world's societies (Mitrovic et al, 2013; Yihua et al, 2013). Digital inclusion programmes are therefore vital in bridging both the digital and social divide (Mervyn, 2014; Powell, 2011). Digital inclusion can be approached in two ways, reducing the exclusion or simply enhancing inclusion.

Groups vulnerable to exclusion

This study shall be seeking to establish, how security usability affects access to, usage of and benefits from eservices among the vulnerable groups. Many researchers have identified the most vulnerable as the socially excluded (Bosch et al., 2010; Charleson, 2012; European Union, 2014) including the elderly, people living with disabilities, the poor, those with low literacy levels and those who do not speak English (Lue & Dooley, 2009).

The elderly are digital marginalization in many fronts. A research by Age Uk (2012) found that the elderly are digitally excluded because of, among other factors, usability issues, training and support and internet security issues. Most of them have retired, with little finances and thus not able to afford or access the services. Some are ailing and in need of health care. Health management system would come in handy for them. Inability to access makes them marginalized. In developing country like Kenya, most of the elderly are not educated. As such, the lack the skills to use the technology and they are also slow to learn to use the technology. Most of them rely on help from others in using e-services. If the services are sensitive, like health or money transactions, there is the risk that people they seek help from can expose them or even steal from them. Most of them especially from the rural areas can only communicate in their mother tongue. It means they are not able to interact with the system effectively. There is need to design systems that can have them enjoy the services. A security mechanism that is usable and friendly to them to enjoy the services without the risk of fraud from those they seek help from.

People living with disability are also marginalized in many fronts as well. In the digital inclusion debate, the blind for instance are able to use computers aided by screen readers (Singh, 2012). These readers speak to the user the contents of the screen. Most of the e-services however have not adopted this technology (Hink & Alcides, 2010). The risk, however, is that the computer may speak your pin or password as you type it and hence expose the user to cyber crime. There is need for a security system that the blind can use to input their secret without the fear that someone else is listening. This may involve software designs, special hardware and even the environment, like a sound proof both for the blind. There is not much research done on security vulnerability among the blind users.

The illiterate and the not highly education in the society have problems using the computers and e-services (Chavan, 2012). Alshehri et al (2012), identifies lack of knowledge and ability to use computers as a major barrier. Many such users often say they don't need the computer based services. Those who get exposed to the systems properly however are able to embrace the technology. One of their concerns is security and just like the elderly, they risk fraud because they rely a lot on help from others. The denial of the need to use computers is an indication of despair and ignorance. "Accuracy, security, network speed, user-friendliness, user involvement and

convenience" are "the most important quality attributes in the perceived usefulness of Internet-based e-retail banking" (Alsmadi, 2011; Saarenpaa, 1997). Using text and numbers as the passwords blocks this group from accessing and using the services. There is a need to see whether other alternatives such as diagrams, pictures or barcodes can improve their use experience positively. This group is also highly vulnerable to social engineering based attacks. Language barrier is also a significant factor in digital exclusion. Many services especially in Kenya are English based. Most the elderly and the lowly educated have inadequate knowledge and understanding of English language. A friendlier system would consider having language that users are familiar with especially where feedback is needed. For instance, an MPESA transaction could have a Swahili message confirming its conclusion.

Reducing exclusion involves overcoming the barriers to inclusion. According to Sen's Capability approach (Nyambura & Waema, 2011), the welfare of human life can be analyzed in terms of individual capabilities and functioning (Iep, 2014). While the Functionings are achievements, the capabilities are the abilities to achieve them (Zheng & Stahl, 2011). Functionings are states of being and doing. It is what an individual is or is doing such as owning a mobile phone, transacting an e-service, being e-skilled, participating in elections, being malnutrition or being healthy. Capability on the other hand is the set of valuable functioning that a person has effective access to (IEP, 2014). Here we look at what choices an individual has on what functioning to achieve. For instance, a person Y chooses to queue in the bank hall to withdraw money because the line in the ATM is equally long and besides he may enjoy a sitting break in the banking hall even as he waits for the queue to move. Another person X has to queue in the banking hall as well but because he is not able to use the ATM. The ATM's interface is designed in English for instance and would require her to input her PIN in order to complete the transaction. Person Y, being illiterate and English not being her first language, will have to disclose her PIN to a stranger and risk being fraud or cannot simply use the ATM. While X and Y are basically doing the same thing (functioning), Y is doing it more out of choice while X on the other hand is doing it more for lack of an alternative choice. X has no ability to achieve an ATM transaction (Mitrovic et al., 2013). As a result of this inability, X has to incur higher charges for over the counter withdraws, endure long queues in the banking hall, and may have to travel to the bank premises possibly leaving an ATM facility in her neighborhood. This is a clear case of inequality.

In most research on usability security, the target is the common user. The researchers seek to improve the experience of the standard user. There is need to establish whether the findings and recommendations would apply to the vulnerable groups as well. This study seeks to fill that gap.

SECURITY

Systems Security

An important aspect of e-services, in the view of many researchers is system security (Chavan, 2012; Rehman et al., 2012; Barrera, et al., 2010; Upadhyaya. et al., 2012).System security is the broad area concerned with the threats posed by use of ICT (Shava & Greunen, 2013). According to Hong et al., (2003) among issues covered in security include contingency planning, policies on information security, risk analysis and management and disaster recovery. The core concerns in security are availability, integrity and confidentiality (Hong Kwo-Shing, et al., 2003; Wang, 2009; Kulkarni, 2010; Cristea et al., 2012). Braz et al (2013) calls them the three essential security properties (confidentiality, integrity, and availability) that distinguish authorized and unauthorized users.While some researchers have laid more emphasis on the availability, integrity and confidentiality of data (Kulkarni, 2010) and information (Wang, 2009), others emphasizes on the integrity and confidentiality of business procedures (Hong et al., 2003) yet others on the availability, integrity and confidentiality e-services platforms (Cristea et al., 2012).

E-Services are vulnerable to various kinds of threats ranging from the attacks from the internet to the errors by legitimate users (Cristea et al., 2012). An e-service platform should ensure security for both the provider and the client as both are vulnerable to cyber crime among other security risks (Tariq & Arif, 2014). Accessing electronic services often requires that the user and the system exchange information. The system stores sensitive data about the client. If this data falls on the wrong hand, it may be used to commit crime such as fraud and identity theft that may hurt the client (Neppe, 2008; Upadhyaya et al., 2012; Tariq & Arif, 2014). On the other hand non authorized access to the system may also lead to stealing of data about the organization and consequently loss of money, privacy and confidentiality (Bansa & Zahedi, 2014). It is therefore important that the organization protects its own data and system from unauthorized access. Security mechanisms are aimed at detecting and preventing unauthorized activities or threats as well as reducing the impacts should these threats succeed. To ensure security is acquired, systems, operations and internal controls should be combined to ensure integrity and confidentiality of the data.

Security is both a challenge and a blessing in ensuring the uptake of digital platforms. It can determine the success or failure of an E-service platform. Chavan (2012) identifies security as a major challenge in e-banking. Alshehri et al. (2012) identifies poor security and privacy mechanisms among infrastructure and lack of capacities as the major barriers to use of e-government services by citizens. Among other barriers to e-services include lack of knowledge and ability to use computers. Many other researchers assert that lack of security and privacy erodes users trust in online systems (Wang, 2009; Conklin, 2007).A good system with good services can be irrelevant if users fail to trust it (Wang, 2009; Alshehri et al., 2012). It is important that clients are not only able to use the system but also trust the system (Turel

and Gefen, 2013). Security is critical in building this trust (Rehman et al., 2012). E-Services should therefore offer "confidentiality, integrity, and availability to users and other e-Services" (Cristea et al., 2012).

While most of the research has identified security as a barrier to offering, accessing and using E-services, Most of the research has focused on the challenges in implementing security. The emphasis have been on making the system more secure as opposed to empowering those barred to overcome the barriers. Very little however have been done to address the plight of those barred from accessing the system by security.

Security threats in systems

How security is implemented in a system largely depends on, among other factors, the threats that the system is exposed to and whether the threats, according to Alsmadi (2011), are technical or non technical.

Technical threats

Technical security in E-services can be viewed to have three layers as identified by Upadhyaya et al. (2012). The first is Application layer it deals with "Authentication, data integrity, trust, user anonymity and security dependencies" Upadhyaya et al. (2012). The second is the Network layer security. It is concerned with cryptographic methods and protocols for safe internet communications Alfayyadh et al (2010). The third is Data security layer which includes protecting the database and the files that contain data. This may include back up, recovery techniques, and passwords on documents among other methods Upadhyaya et al. (2012).

We can also look at Technical security from its five components as described by Alsmadi (2011); a) Unauthorized access; this is characterized by users accessing more than they are privileged to access (Singh and Chauhan, 2012). b) Loss of integrity; where data could produce invalid results or be modified by the wrong persons. c) Loss of availability; leading to denial of service. d) Exploitation of data; where personal information may be used for wrong reasons other than what it was gathered for, and e) Authentication and accountability; this concerns issues like who should add or upgrade users.

At the Technical security level the three security properties; confidentiality, integrity, and availability are assured through authentication Braz et al., (2013).

Non technical threats

Aside from technical threats non-technical threats include among other things legal issues and qualification criteria to access services (Alsmadi, 2011). It is about the people's roles in protecting the information, data and processes. Wang (2009) acknowledges the shifting role of security from purely technical to include people as well. Even Dan and Dan (2013) assert that computer security is not just technical but a people's problem as well (Gollman, 2011). It is about how people interact with security systems. For effective security, proper use of security mechanism is paramount hence "Mechanisms and models that are confusing to the user will be misused" (Zurkos, 1996). In an e-government site for instance a few questions may be asked. Does the system disallow non citizens from applying for National Identification Card? How reliable is the information availed by the site? According to Kainda et al (2010) security has been so much about attackers and entities with malicious intents. Attackers can be from within the system or external (Alsmadi, 2011). They also point out that even non malicious users can compromise security if poorly managed. The organization should ensure people comply with security policies. Otherwise, as Alfayyadh and Josang (2010) points out, an improperly managed security system is likely to cause more harm than no security at all.

System Usability

Just like security, usability is a critical aspect in adoption of e-services (Rehman, Coughlan & Halim, 2012). Security alone without usability is not sufficient to building trust among users of online services. Usability is an equally important component of trust (Wang, 2009). A software product that fails to "incorporate proper usability, security and efficiency in system design" is likely to be completely rejected by users (Rehman et al., 2012). Sambhanthan and Good (2012) asserts that web usability is critical in triggering a positive user experience, a vital requirement in e-commerce (Omar et al., 2013; Nilashi et al., 2011). Whether to buy online, transfer money, renew a license online or access other government services, a positive user experience will always motivate the user to use the e-service. It is part of the trust that users develop towards an online seller (Wang 2009). Customers are likely not to return to a site that lacks positive user experience (Sambhanthan & Good, 2012). According to Omar et al. (2013) poor usability of e commerce applications and the consequent lack of trust on online transactions have denied many organizations an opportunity to enjoy the benefits of e-commerce. To Omar, "usability is a very important condition for survival of websites" and people leave if the website is not usable or is difficult to use (Omar et al., 2013). System usability concerns include issues such as how easy a user is able to accomplish a task as required using the system, how long (time taken) to performing a task, learnability of the system or process (how easy for users to learn to use), how much help required and frequency to seek help when using, need to remember (vis-a-vis recognition) among other aspects. Usability issues are addressed either through interface design or the underlying system model (Reeder et al., 2011)

Usability and security

Most researchers have looked at usability and security as separate issues that influence access and use of e-services (Sahar, 2013). It is an approach that has brought its share of challenges in design, adoption and use of e-services. The security and usability design processes are spear headed by two different teams with different philosophies and goals that are always conflicting. While usability seeks to simplify access to services, security seeks to make it hard for the

unauthorized user to access the system (Kulkarni, 2010). Usability is designed for even the novice users to easily navigate the system while security is aimed at making even the most experienced user unable to navigate the system when not authorized. The usability philosophy is easy to use and navigate, that of security is hard to crack or penetrate (Kainda et al., 2010). This has led to most secure systems not to be user friendly. Usable systems are often said to be less secure. Many researchers have actually argued that secure systems cannot be usable (Alsmadi, 2011; Vallee, 2013; Sahar, 2013) and that usability cannot be achieved without compromising security. Others seem to suggest that the best that can be achieved is at least to balance with tradeoffs from both sides. These researchers however fail to acknowledge that an unusable system is not secure. Users abandon unusable systems (Omar et al., 2013; Alsmadi, 2011). This means services and resources offered through the system become unavailable to them. Worse still, users may bypass the security system (Tariq & Arif, 2014), of course by compromising the system and get exposed to threats. This is especially if they perceive security to be standing on their way to using the system. As a result a "secure" system that is not usable compromises the integrity and availability of the data and resources it had sought to protect.

The solution then is neither making tradeoffs nor in choosing between security and usability but to develop system with usable security. Several researches are being done on how to make security usable however very little is being done on evaluating how lack of usable security could be contributing digital exclusion. It is a considered assumption in this study that taking into account the perspectives of those marginalized could result in to a more usable and readily acceptable security in systems. Security, from the users view, including the marginalized, is the assurance that the user is safe, that the information submitted or acquired by the system is used for the right reasons, that any valuables like money or identity will not be stolen when in the care of the system, and that the transactions carried over the system are real, genuine and will not result into a fraud.

Security, Usability and Digital Exclusion

As debated earlier, security and usability are both components of trust that is a critical factor of adoption of e-services. Unusable security has been identified as a barrier to use and access of e-services consequently leading to digital and social exclusion. Poor security usability is considered a threat to digital inclusion because of the position of security features in the navigation of a system. "Username and password is the first line of defense against unauthorized access to the company's 'resources' " (Kulkarni, 2010) since it is the first thing that a user interacts with before accessing a service. Rehman et al., (2012) looked at usability based cashless payment systems and cited usability issues as "…key inhibitors to the success of electronic payment systems…". They acknowledge the complete traversal by payments card from "conventional cash payment systems to a more secure online payment method" (Rehman et al., 2012). While the cards offer more utility, usability and reliability to the customers, they raised new challenges such as hacking and card theft. They asserted that the slow adoption to cashless payment is related to lack or low usage of Human computer Interaction Principles in the design process. Rehman et al. (2012) recommends the incorporation usability features in system design as well as involving third party and financial institutions to ensure total customer experience in cashless payments.

Social security usability challenges

Steyn and Johanson (2011) in their book "ICTs and Sustainable Solutions for the Digital Divide: Theory and Perspectives" view digital inclusion as incorporating digital divide and social inclusion. They argue that "Treating 'digital inclusion' from the field of Social Policies demands the discussing of issues that are usually taken for granted, or less discussed (Steyn & Johanson, 2011) Cushman (2008) also asserts that problems of technology arise from earlier studies that had ignored the threat posed by technology adoption to social inclusivity. According to Steyn and Johanson (2011), we cannot address'digital inclusion' concepts without considering social inclusion and exclusion theories. To them, theoretical approaches on digital inclusion vary according to different understandings about:-

(a) society and social dynamics;

(b) State,market, civil society relationships and the role of public policies;

(c) the purpose(s) of disseminating digital information and communication technologies (ICT), which are usually related to neologisms such as 'Information', 'Knowledge' or'Network' Societies;

(d) the reciprocal influence of each one of these aspects to one another, and how they connect to form different frameworks to approach 'digital inclusion" (Steyn & Johanson, 2011) with Post moderm theories having culture and identity as well as ICT as crucial elements for analyzing and theorization social dynamics

Technical security usability challenges

Most e-services are offered in distributed systems. According to Cristea et al. (2012) the decentralized nature of distributed systems, remote access by users and its distribution over large geographical areas make it more vulnerable to threats. Besides, Cristea et al. (2012) argues, distributed systems extend over multiple administrative domains whose security policies are different. They are shared by different user groups and are operated at both local and global levels. All this makes implementing e-services security implementation challenging. According to Singh and Chauhan (2012) the complexity of data security increases as data becomes more valuable "While the data-sharing trends offer improved means of governance, these same trends make them even more vulnerable to hackers, a prey to performance issues" (Singh & Chauhan, 2012). Alsmadi (2011) discusses security as a key challenge in expanding e-government services. According to Wang (2009) "identifying users, authenticating users, storing public and classified information in same websites, checking authorizations, auditing, signing

transactions, resolving conflicts, keeping copies of information" are the security challenges in e-government services.

Wang notes that, in paper based systems, security threats had been identified over a long time, analyzed resolved through robust policies and procedures (Wang, 2009). Replicating the same in digital systems could be important but has not been as easy. "Solutions for problems such as global identity management, cross boarding identification, privacy, prevention of attacks are essential for the wide public acceptance of e-Services " (Cristea et al., 2012). Different attempts to uniquely identify e-services users digitally have been made. In deed Digital identification according Alsmadi (2011) "is increasingly evolving in use and importance as a method to safely identify humans or entities especially through on-line business transactions". However, writing signatures still remains a requirement for verification in many e-service provisions. It is Alsmadi (2011) view that biometric signatures have the potential to solutions but as at now, they can't be employed to conveniently enable fast transactions and with reasonable cost.

As was noted in section earlier, security has both technical and people oriented dimensions. Designing secure and robust mechanism is challenging enough. But even the best designed security systems needs to be implemented and configured right for them to be effective. Using the existing security mechanism as they are meant to be used has also been a challenge. For instance, just as passwords have been identified as the mostly used form of authentication (white & Shaw, 2014) they have also been shown to be the easiest system to compromise (Sahar, 2013). This is due to the tendencies for users to choose weak and convenient password (Shava & Van Greunen, 2013). A good password should be easy to remember but hard for someone else to guess (Jebriel, 2014). The bad choice of passwords by users have been attributed to several factors among them; having many internet accounts hence the memory load increases, not understanding the risks thus being less careful and lack of password policy by the services provider (Tariq & Arif, 2014). Other risky behavior includes exposing the passwords by sticking them on the computer screens or note books. Making security usable is and has been a major challenge in digital systems (Zurko and Simon, 1996).

Usable Security

A new relationship between usability and security is seemingly emerging. Like two Siamese twins, it is increasingly requiring that you do not have one without having the other for secure systems. National Academy of Science (2010) acknowledges that with more-usable security the inadvertent and sometimes deliberate undermining of security can be avoided. They contend that "Indeed, without sufficient usability to accomplish tasks efficiently and with less effort, users will often tend to bypass security features". We therefore can no longer afford to approach security and usability separately. Usability should be considered part of security. Security experts should be equipped with Human Computer Interaction (HCI) skills (Rehman, Coughlan & Halim 2012). The need to have usable secure systems is becoming apparent and is generating interest among researchers (Vallee, 2013; Sahar, 2013). One of the approaches being adopted is using HCI principles in security mechanisms (Rehman, Coughlan & Halim, 2012). According to Reeder et al. (2011), "Usability improvements to security systems, such as access control systems, can come from two sources: improvements to user interfaces and changes to underlying system models".

Most researchers have focused on usable authentication systems. Authentication is part of a broader security measures in protecting both the clients and the enterprises data (De Cristofaro, 2014). It is the process of establishing whether a user is who (s)he claims her/himself to be and it is usually interactive (Braz et al., 2013). Authentication involves a secret (Dan & Dan, 2013) stored in the system. The user provides a similar secret to the system. If the secrets match, then the user is allowed access to the resources.

Use of passwords, a simple and practical system understood well by both users and administrators (Dan, 2013) is one of the oldest and most popular forms of authentication (Denning, 1992; De Cristofaro et al., 2013; Dan & Dan, 2013; White & Shaw, 2014). Many authors actually use authentication and password interchangeably. A password consists of any length of a sequence of characters from a pool of allowed characters, used to authenticate a user (Bosworth & Summers, 2004; Dan & Dan, 2013). They however have many short comings (Orman, 2013) despite their dominance (Inglesant & Sasse, 2010; Dan & Dan, 2013) and popularity. Short passwords however are insecure, easy to guess and vulnerable to brute force attack. The security of a password can be increased by making it long, eight characters and above (Ars Technical 2013; Dan & Dan, 2013). This however reduces its usability. Long passwords are hard to remember. A good password should be hard to guess and easy to remember for the users. The security of a password can be enhanced by mixing alphanumerical characters with special characters. The characters should be picked at random. The wide the pool of the characters, the safer the password will be. But this results passwords that are meaningless to the users. With the number of online accounts increasing for each user, the memory load for different meaningless passwords becomes unbearable. Many of them forget especially those not frequently used. Users then tend to choose password that are meaningful. Like a name combined with a birthday. This in turn becomes easy to guess and makes them vulnerable to hackers. This has seen most systems control the type of password users have, either by assigning passwords to users or by guiding users as they pick them. Increasing the security or usability of password clearly reduces the other. Passphrases have been floated as an alternative to passwords. Passphrases are longer than passwords and easier to remember as users can use words that are meaningful to them. They are resistant to brute force attack. But they are however vulnerable to dictionary attacks, An attack similar to a brute force attack only that instead of combinations of character it tests word combinations (Herley et al., 2010).

Among usability issues in password and passphrases are memorability errors and Typographical errors (Dan & Dan,

2013). Typographical errors occur when the user remembers the secret but types it incorrectly. This may occur when the secret for example has symbols replacing alphanumerical characters. It is also caused by masking of secrets by the system to protect eavesdropping. The user is not able to confirm whether the secret put is the correct save for the number of characters. In case of mismatch, the system only error message is that authentication failed (Keith et al., 2009). Word processing mode (WPM) where the password or passphrase are structured very similar to regular words or sentences that are used on a daily bases have been recommended as a possible solution to typographical errors (Keith et al., 2009; Dan, 2013). This will reduce the memory work load, reduce typographical errors and keep the secret long and hence secure.

Memory related errors on the other hand are where users devise ways to ease the memory load and in the process compromise the system. This includes writing passwords on papers, using the same passwords for different accounts and sometimes sharing passwords. The remedy for this includes memorizing the secret until it's stored in the long term memory. This could be by writing it down many times (Keith et al., 2009; Gollmann, 2011). Or let the users select the secrets since user selected secrets are easier to remember (Haga & Zviran, 1992). Other solutions to usability for secret based authentication include single sign-in solutions (Glassman, Tam & Vandenwauver, 2010), allowing users to write passwords down (AlFayyadh et al., 2012), use of pronounceable authentication strings (White and Shaw, 2014) and use of password management software. Most of the discussed usability problems with secret based authentication assume the user is capable of at least reading and writing the secret. The fate of the vulnerable groups has not been adequately researched. The above suggested solutions have not considered the illiterate, for instance, or those not able to use the computers.

Non technical attacks on secret authentication are also a major problem. This includes social engineering attacks (Chantler & Broadhurst, 2006). This is where psychological tricks are used to make users reveal their secrets. Others includes eavesdropping on users or shoulder surfing. This can be remedied through awareness campaigns by service providers and civic education among users. Organizations ought to have security policies that guide users on selection and use of authentication secrets and mechanisms to make sure that these policies are followed and adhered to. Care should be taken to ensure that the policies are friendly and strict enough such that security is ensured without frustrating the users rest they are tempted to compromise the system.

An alternative to passwords and passphrases is the biometric authentication. An image of a users feature such as the finger print or voice is kept on the system (Alsmadi, 2011). The feature is compare with the user to verify and allow him to use a resource. The challenge with this authentication is that it's still not fully developed to be reliably used in every day transactions, it's expensive and it's affected by factors like illness which may affect the captured features.

Several other solutions have been proposed in dealing with usable security (Braz et al., 2013). They include graphical passwords (Dunphy & Olivier, 2012) multifactor security (De Cristofaro et al., 2013), guiding clients when selecting passwords (Tariq & Arif, 2014), use of password management systems (Stajano, 2014) among others.

Tariq and Arif (2014) identified three levels of usable authentication. The First level is presence of strong password rules that users must comply with during sign up "i.e. accounts security at the time of account creation" The Second level is on account recovery, if a user lost the account, like forgets password or user name, it should be easy and safe for the user to recover it. Third level concerns password session time-out, it includes the need to change the password.

Alfayyadh et al. (2010) outlined eight security usability principles, grouped into security action principles and security conclusion principles. A security action is when users are required to produce information and security tokens, or to trigger some security relevant mechanism. Like during authentication. The security action principles include:

the users must understand which security actions are required of them

the users must have sufficient knowledge and the practical ability to make the correct security action

the mental and physical load of a security action must be tolerable and

the mental and physical load of making repeated security actions for any practical number of transactions must be tolerable.

A security conclusion is when users observe and assess some security relevant evidence in order to derive the security state of systems like when an SMS is sent to confirm an Mpesa transaction. The Security conclusion Usability Principles include:

The user must understand the security conclusion that is required for making an informed decision. This means that users must understand what is required of them to support a secure transaction.

The system must provide the user with sufficient information for deriving the security conclusion. This means that it must be logically possible to derive the security conclusion from the information provided.

The mental load of deriving the security conclusion must be tolerable.

The mental load of deriving security conclusions for any practical number of service access instances must be tolerable.

E-services enhancement of social exclusion

In the light of ICTs role in development, inability to use or access the technology would cause marginalization. "It is not

a viable option to remain offline in today's world…those with limited access to technologies or limited digital literacy skills are at a social disadvantage" (Visser, 2012) Yang also states that "if ICT is only available to some groups of individuals in the society then there will be automatically unequal economic growth within the very community. The resulting disparity in access to ICT is likely to lead to income inequality and poverty" (Yihua Yang et al., 2013). According to Cushman (2008) the most recognized of the ICT related problems "has largely been confined to disruption in the work place and the risk to organizational effectiveness posed by poor designed and implemented systems" but after internet use came in to performing a majority activities then excluded some people from mainstream economic and cultural activities (Cushman, 2008). A clear cycle of interdependence between social exclusion and digital exclusion is emerging from literature as illustrated in fig 1-1.

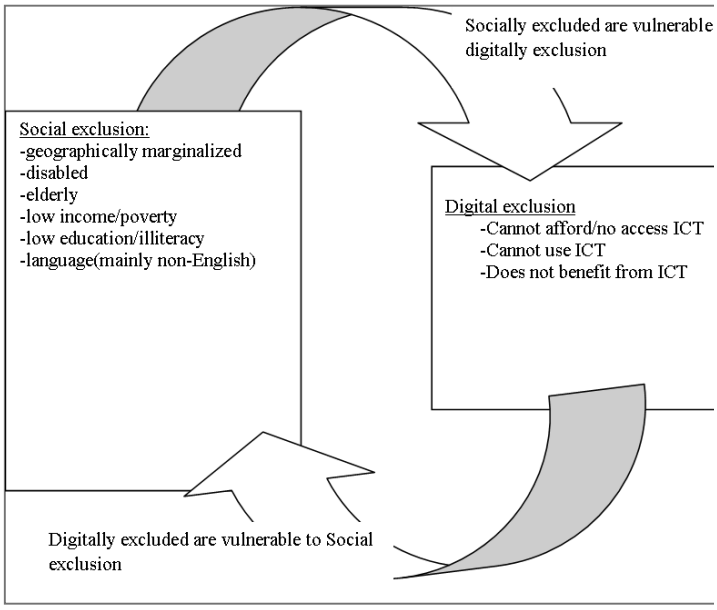

Figure 1-1: the digital and social exclusion vulnerability cycle.

(Source: deduced from literature review by author)

The socially excluded are more vulnerable to digital exclusion and those excluded digitally are likely to be socially excluded especially in the new information age where more and more information and services are becoming available in digital form (Bosch et al., 2010). A Chartered Institute of Taxation (CIT) in UK on digital exclusion showed, among the key findings, that a significant proportion of the population is digitally excluded because they lack access or have low digital literacy skills. Exclusion is more than just access to the computer, motivational factors are a barrier to inclusion as people don't use the services and prefer the traditional systems even when they have access. "Digitization of government services could reinforce social exclusion of a sizeable segment of population" (CIT, 2012). The report had among its recommendations that digitization should take an inclusive approach, that digital policy should focus on bringing the excluded on board where possible by assisting and encouraging. It also recommends that the online services be made as simple as possible (CIT, 2012). Chavan (2012) identifies security as a major challenge in E-banking He says that it will be essential "for example… to define an electronic signature and give same legal status as the hard written signatures…" Other factors included, positive user experience which helps to build trust (Alshehri et al., 2012). Lack of trust would make citizens reject the services. Visser says that "the ability to successfully navigate often complex websites and online systems determines if a person will be able to apply for assistance, schedules meetings or download a tax form" (Visser, 2013)

SUMMARY

This paper has discussed the e-services concept and its contribution to digital exclusion. It explored security, usability, and the contribution of security usability to digital exclusion. The paper finally discussed how usability is contributing to the digital exclusion that is enhancing social exclusion.

When security stands on the way to using the system, the user is likely to either bypass the security system (Tariq & Arif, 2014), of course by compromising the system or abandon the system (Alsmadi, 2011). There are people who are likely to be affected by unusable security more than others (UN, 2012) due to one or more characteristics that they may have. These are people who, because of being disabled, of a certain age, low education level, belonging to certain economic status, from a certain geographical location or even unable to understand English for instance, are likely to not use the system because of security usability. There isn't much research on how security usability may affect e-service provision among these vulnerable groups. Some of the solutions advocated for security usability may not apply for these groups.

REFERENCES

Al Fayyadh B., Ponting J., Alzomai M. and Josang A. (17-19 December 2010). Vulnerabilities in personal firewalls caused by poor security usability. In Fan, P & Yuan, D (Eds.). Proceedings of the 2010 IEEE International Conference on Information Theory a and Information Security. China.

Alshehri M, Drew S and Alfarraj O. (2012). A Comprehensive Analysis of E-government services adoption in Saudi Arabia: Obstacles and Challenges. (IJACSA) International Journal of Advanced Computer Science and Applications , 3(2):1-6.

Alsmadi I. (2011). Security Challenges For Expanding E-governments' Services. International Journal of Advanced Science and Technology , 37: 47-60.

American Library Association. (2012). Public libraries & digital inclusion. Digital Inclusion Survey. The Information Policy and Access Center (IPAC) and the International City/County Management Association (ICMA).

Animashaun J. O, Fakayode S. B, Idris K. A and Adedokun K. F. (2014). 1.Patterns and Drivers of Mobile Telephony for Sustainable Livelihood among Farming Households in Kwara State, Nigeria. Journal of Agricultural Informatics , (5)2:34-44.

Ars Technica. (2013, 10 16). How the Bible and YouTube are fueling the next frontier of password cracking . Retrieved from Ars Technica: http://arstechnica.com/security

Bansal G And Zahedi F M. (2014). Trust-discount tradeoff in three contexts: frugality moderating privacy and security concerns. Journal of Computer Information Systems .

Bansode S.Y. and Patil S.K. (2011). Bridging Digital Divide in India: Some Initiatives . Asia Pacific Journal of Library and Information Science , 1:1.

Barrera D., H. Güne ̧s Kayacık H. G., van Oorschot P.C.and Somayaji A. (2010). A Methodology for Empirical Analysis of Permission-Based Security Models and its Application to Android. ACM 978-1-4503-0244-9/10/10 .

Bosch, w. v., & jan dekelver, J. E. (2010). incluso: social software for inclusion of marginalized youth. Journal of Social Intervention: Theory and Practice , 19 (4), 5-18.

Bosworth E. and Summers W. C. (2004). Password policy: the good, the bad, and the ugly. Proceedings of the winter international symposium on Information and communication technologies (WISICT '04).

Braza C,Porriera Pe, and Seffahb A. (2013). Designing Usable, Yet Secure User Authentication Service: The Cognitive Dimension. University of Montreal, Canada: Dept. of Computer Science .

Bunker B. (2010). A Summary of International Reports, Research and Case Studies of Digital Literacy: Including implications for New Zealand of adopting a globally-recognised digital literacy standard. New Zealand Computer Society.

Carter L. and Bélanger F. (2005). The utilization of e-government services: citizen trust, innovation and acceptance factors. . Information Systems Journal , 15(1):5–25.

Chantler A. N. and Broadhurst R. (2006). Social engineering and crime prevention in cyberspace. Brisbane: Queensland University of Technology.

Charleson, D. (2012). Bridging the digital divide: Enhancing empowerment and social capital. Journal of Social Inclusion , 3 (2), 6-19.

Chavan J. (2013). Internet banking- benefits and challenges in an emerging economy . International Journal of Research in Business Management (IJRBM) , 1(1): 19-26.

Conklin, W. A. (2007). Barriers to Adoption of e-Government. System Sciences. HICSS 2007. 40th Annual Hawaii International Conference on system sciences. Hawaii: IEE.

Cristea A., Hummels D. and Roberson B. (2012). Estimating the Gains from Liberalizing Services Trade: The Case of Passenger Aviation. mimeo: University of Oregon, .

Cushman M. and McLean R. (2008). Exclusion, inclusion and changing the face of information systems research. Information, Technology and People , 21 (3): 213-221.

Cushman, M., & McLean, R. (2008). Exclusion, inclusion and changing the face of information systems research. Information Technology & People , 21 (3), 213-221.

Dan A. and Dan S. (2013). Authentication with Passwords and Passphrases -Implications on Usability and Security. Lund University School of Economics and Management (Lecture notes).

De Cristofaro E, Du H, Freudiger J, and Norcie G. (2013). A Comparative Usability Study of Two-Factor Authentication. www.internetsociety.org/sites/default/files/01_5-paper.pdf.

Denning P. J. (1992). The Science of Computing: Passwords. A. merican Scientist, , 80(2): 117-120.

Dunphy P and Olivier P. (2012). On Automated Image Choice for Secure and Usable Graphical Passwords. ACSAC ’12 Proceedings of the 28th Annual Computer Security Applications Conference (pp. 99-108). New York, NY, USA: ACM .

Fuchs, C., & Horak, E. (2006). Africa and the digital divide. Telematics and Informatics , 25 (2008), 99–116.

Glassman M., Tam L. and Vandenwauver M. (2010). The psychology of password management: a tradeoff between security and convenience. Behaviour & Information Technology , 29 (3): 233-244.

Gollmann, D. (2011). Computer Security, 3 rd ed. . John Wiley & Sons.

Graham M. (2011). Time Machines and Virtual Portals: The Spatialities of the Digital Divide. Progress in Development Studies , 11(3):211-227 .

Green M and Rossall P. (2013). Digital inclusion evidence review. Age Uk.

Haga W. J. and Zviran M. (1992). A comparison of password techniques for multilevel authentication mechanisms. The Computer Journal , 36 (3).

Hellman R. (2008). Accessibility of eservices on mobile phones. . IADIS International Conference e-Society (pp. 263-270). Algarve, Portugal: International Association for Development of Information Society.

Herley C., Mitzenmacher M.and Schechter S. (2010). Popularity is everything: a new approach to protecting passwords from statistical -guessing attacks. Proceedings of the 5th USENIX conference on Hot topics in security (HotSec'10).

Hick, C. P. (2008). Moving From Digital Divide to Digital Inclusion. Currents: New Scholarship in the Human Services , 7 (2), -.

Hink, R. B., & Alcides, a. s. (2010). Basic Human Computer Interface for the blind. Innovation And Development For Americas (p. 1). PERU: 8th Latin America and Caribbean conference engineering and Technology(LACCEI).

Hong K, Chi Y, Chao L. R, and Tang J. (2003). An integrated system theory of information security management. Information Management & Computer Security , 11(5): 243 - 248.

Inglesant P. G. and Sasse M. A. (2010). The true cost of unusable password policies: password use in the wild. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10).

Jibril, T. A., Tan, B. H., & Mohammed, S. (2014). Potentials of Global Networking in SMS Technology: An Example of Nigerian Users. Online Journal of Communication and Media Technologies , 4 (2), 51-72.

Kainda R, Flechais I, and Roscoe A W. (2010). Security and usability: analysis and evaluation . Proceedings Fifth International Conference on Availability, Reliability and Security (ARES 2010, (pp. 275-282). Krakow, Poland.

Karume, S. M., & Mbugua, S. (2012). Trends in Adoption of Open Source Software in Africa. Journal of Emerging Trends in Computing and Information Sciences , 3 (11), 1509-1515.

Keith M., Shao B. and Steinbart P. (2009). A Behavioral Analysis of Passphrase Design and Effectiveness. Journal of The Association For Information Systems , 10(2): 63-89.

Kieran M, Simon A. and David K. A. (2014). Digital inclusion and social inclusion: a tale of two cities. Information, Communication & Society , 17(9):1086-1104.

Kulkarni D. (2010). A Novel Web-based Approach for Balancing Usability and Security Requirements of Text Passwords. International Journal of Network Security & Its Applications (IJNSA) , 2(3):1-16 .

Lor C. K. (2003). Factors Leading Hmong Youth To Join Gang. . Masters thesis of University of Wisconsin-Stout.

Luke, Allan and Dooley, Karen T. (2009). Critical literacy and second language learning. In E. E. Hinkel, Handbook of Research on Second Language Teaching and Learning Vol. 2,. New York: Routledge.

Marvin, C. . (1988). When Old Technologies Were New: Thinking About Electric Communication in the Late Nineteenth Century. New York: Oxford University Press.

Michalski . R, Jankowski. J. and Kazienko . P. (2012). Negative effects of incentivized viral campaigns for activity in social networks. Proceedings of the 2nd International Conference on Social Computing and its Applications, SCA 2012 (pp. 391-398). Xiangtan, China: IEEE Computer Society.

Minichiello V, Rahman S, Dune T, Scott J and Dowsett G. (2013). E-health: potential benefits and challenges in providing and accessing sexual health services. BMC Public Health 2013, 13:790 doi:10.1186/1471-2458-13-790 .

Mitrovic Z. (2013). E-social Astuteness skills for ICT-supported equitable prosperity and a capable developmental state in South Africa. International Journal of Education and Development using Information and Communication Technology (IJEDICT) , 9(3): 103-123.

Montagnier, P. a. (2011). "Digital Divide:From Computer Access to Online Activities – A Micro Data Analysis. OECD Digital Economy Papers. no 189: OECD publishing.

Neppe, V. M. (2008). The email security-usability dichotomy: Necessary antinomy or potential synergism? Telicom , 21 (3), 15-31.

Nilashi, M., Ibrahim, O., Barisami, M., Janahmadi, N., & Ithnin, N. (2011). Developing a Framework for Exploring Factors Affecting on Trust in M-Commerce using Analytic Hierarchy Process. Computer Engineering and Intelligent Systems , 2(8): 59-70.

Nyambura M. and Waema T. M. (2011). 26. Development outcomes of internet and mobile phones use in Kenya: the households' perspectives. Emerald Group Publishing Limited.

OECD. (2001). Understanding The Digital Divide. Paris : OECD.

Omar, H. F., Saadan, K., & Hamad, O. S. (2013). Review: The Development of a Trustworthy Framework in E-Commerce Applications In Developing Countries. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering , 2 (6), 2086-2088.

Orman H. (2013). Twelve random characters: passwords in the era of massive Parallelism. . IEEE Internet Computing , 17(5): 91-94.

Powell A. (2011). Metaphors for democratic communication spaces: How developers of local wireless networks frame technology and urban space. Canadian Journal of Communication , 36(1): 91-114.

Reeder, R. W., Bauer, L., & Cranor, L. F. (2011). More than Skin Deep: Measuring Effects of the Underlying Model on Access-Control System Usability. CHI. Vancouver, BC, Canada.: ACM.

Rehman, S. , Coughlan, JL. and Halim, Z. (2012). Usability based Reliable and Cashless Payment System (RCPS). International Journal of Innovative Computing, Information and Control , 8 (4):2747 - 2761.

Saarenpaa, A. (1999). Law, Technology and Data Technology.Judicial Academy of Northern Finland. Retrieved from http://www.urova.fi/home/oiffi/julkaisut/lawtech.htm.

Sahar F. (2013). Tradeoffs between Usability and Security. IACSIT International Journal of Engineering and Technology , 5(4): 434-437.

Sambhanthan A. and Good A . (2012). Strategic advantage in web tourism promotion:an e-commerce strategy for developing countries. International Journal of Information Systems in the Service Sector (IJISSS) , 6 (3).

Shava F. B. and Van Greunen D. (2013). Factors Affecting User Experience with Security Features: A Case Study of an Academic Institution in Namibia. Information Security for South Africa , 1-8.

Singh A. J and Chauhan R. (2012). Technology Challenges in E-Service Accessibility. Journal of Engineering and Technology , 2(1):32-40.

Singh R. (2012). Blind Handicapped Vs.Technology: How do Blind People use Computers? International Journal of Scientific & Engineering Research , 3(4):1-5.

Singh, R. (2012). Blind Handicapped Vs.Technology: How do Blind People use Computers? International Journal of Scientific & Engineering Research , Volume 3 (issue 4), -.

Smith L. M., Spence R., and Rashid T. A. (2011). Mobile Phones and Expanding Human Capabilities. USC Annenberg School for Communication & Journalism , 7(3): 77–88.

Stajano, F., Jenkinson, G., Payne, J., Spencer, M., Stafford-Frasser, Q., & Warrington, C. (2014). Bootstrapping adoption of the Pico password replacement system. Proceedings of Security Protocols Workshop. Springer LNCS.

Steyn J and Johanson G. (2011). ICTs and Sustainable Solutions for the Digital Divide: Theory and Perspectives. New York: Information Science Reference (an imprint of IGI Global).

Tam, L., Glassman, M. and Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. Behaviour and Information Technology , 29 (3):233-244.

Tapia, A. H., Kvasny, L. and Ortiz, J. A. (2011). A critical discourse analysis of three US municipal wireless network initiatives for enhancing social inclusion. Telematics and Informatics , 28: 215–226.

Tariq Z and Arif A. (2014). Usability Analysis on Security of E-mail Accounts: Differences between Fantasy and Reality . International Journal of Security and Its Applications , 8(5):85-96.

The Chartered Institute of Taxation(CIT). (2012). Digital Exclusion. London: The Chartered Institute of Taxation.

Turel O. and Gefen D. (2013). The dual role of trust in system use. Journal of Computer Information Systems , 54(1):2-10.

United Nations. (2012). Bridging the digital divide by reaching out to vulnerable populations. In Chapter 5 in United Nations E-Government Survey 2012 - E-Government for the People (pp. 87-99). United Nations.

Upadhyaya, P., Shakya, S. and Pokharel, M. (2012). Information Security Framework for E-government Implementation in Nepal. Journal of Emerging Trends in Computing and Information Sciences , 3(7): 1074-1078.

Vallee H. Q., Walsh J. M., Zimrin W., Fisler K. and Shriram S. (2013). Usable security as a static-analysis problem: modeling and reasoning about user permissions in social-sharing systems. Proceedings of the 2013 ACM international symposium on New ideas,symposium on New ideas, new paradigms, and reflections on programming & software (pp. 1-16). New York, NY, USA: SIGPLAN ACM Special Interest Group on Programming Languages.

Visser M. (2013). Digital Literacy and Public Policy through the Library Lens. Maine Policy Review , 22(1): 104 -113.

WANG, J.-f. (2009). E-government Security Management: Key Factors and Countermeasure. Fifth International Conference on Information Assurance and Security (pp. 483-486). IEEE.

White, A. M., Shaw, K., Monrose, F., & Moreton, E. (2014). Isn't that Fantabulous: Security, Linguistic and Usability Challenges of Pronounceable Tokens. NSPW 2014 Pre-Proceedings. University of North Carolina at Chapel Hill.

Yang Y., Hu X., Qu Q., Lai F., Shi Y., Boswel, M. and Rozelle S. (2013). Roots of Tomorrow's Digital Divide: Documenting Computer Use and Internet Access in China's Elementary Schools Today. China & World Economy , 21: 61–79. doi: 10.1111/j.1749-124.

Zheng W. and Stahl B. C. . (2011). Technology, capabilities and critical perspectives: what can critical theory contribute to Sen's capability approach? Ethics and Information Technology , 13: 69-80.

Zurko M. E and Simon R. T. (1996). User-centred security. NSPW'96: proceedings of the 1996 workshop on new security paradigms (pp. 27-30). New York NY USA: ACM press.

Authors' Profiles

Mr. Muchiri M. Njoki was born at Kiambu in Kenya on 13th February 1977. He is a PhD candidate in Information Technology at Kibabii University in Bungoma County (Kenya). He has an MSc (Computer Based Information Systems) from University of Sunderland (UK) and a BEd (Science) from Kenyatta University, Nairobi (Kenya). He is an assistant lecturer, Information Technology department and the Deputy Director E-Learning Center at Dedan Kimathi University of Technology (DeKUT), Nyeri (Kenya). He has also been a Mathematics and Physics teacher. Mr. Muchiri's research interests include, digital inclusion, ICT for Development, and Education and ICT. Mr. Muchiri is a member of the Internet Society Kenyan Chapter.

Dr. Franklin Wabwoba is a Senior lecturer in Information Technology and Dean of the School of Computing and Informatics at Kibabii University (Kenya). He holds a PhD (Information Technology) from Masinde Muliro University of Science and Technology, Master of Science (Computer Applications) from Kenyatta University; Endorsement (Educational Management) from University of South Africa and Bachelor of Education (science: Mathematics and Computer Science) from Egerton University. He has taught Computer Science and Information Technology courses for many years. He has ICT industrial experience having worked with Mumias Sugar Company. He has presented several papers in scientific conferences and has many publications in referred journals as well as university level computing books. He has a strong research interest in green ICT, the impact of ICT applications on the community and integration of ICT into education. He is a professional member of the Association for Computing Machinery (ACM).

Dr. Elyjoy M. Micheni is a lecturer in Information Systems and the Chairperson, Department of Management Science and Technology at The Technical University of Kenya. She holds a PhD (Information Technology) from Masinde Muliro University of Science and Technology, Master of Science (Computer Based Information Systems) from Sunderland University, (UK); Bachelor of Education from Kenyatta University; Post Graduate Diploma in Project Management from Kenya Institute of Management. She has taught Management Information System courses for many years at University level. She has presented papers in scientific conferences and has many publications in referred journals. She has also co-authored a book for Middle level colleges entitled: "Computerized Document Processing". Her career objective is to tap computer based knowledge as a tool to advance business activities, promote research in ICT and enhance quality service.