Developing a secured social networking site using information security awareness techniques

Author:
Julius O. Okesola[1]
Marthie Grobler[1]

Affiliation:
[1]School of Computing, University of South Africa, South Africa

Correspondence to:
Julius Okesola

Email:
48948535@mylife.unisa.ac.za

Postal address:
Computer Sciences Department, Tai Solarin University of Education (TASUED), Ijebu-Ode, Nigeria

Dates:
Received: 13 Dec. 2013
Accepted: 11 July 2014
Published: 18 Nov. 2014

How to cite this article:
Okesola, J.O. & Grobler, M., 2014, 'Developing a secured social networking site using information security awareness techniques', *SA Journal of Information Management* 16(1), Art. #607, 6 pages. http://dx.doi.org/10.4102/sajim.v16i1.607

Background: Ever since social network sites (SNS) became a global phenomenon in almost every industry, security has become a major concern to many SNS stakeholders. Several security techniques have been invented towards addressing SNS security, but information security awareness (ISA) remains a critical point. Whilst very few users have used social circles and applications because of a *lack of users' awareness*, the majority have found it difficult to determine the basis of categorising friends in a meaningful way for privacy and security policies settings. This has confirmed that technical control is just part of the security solutions and not necessarily a total solution. Changing human behaviour on SNSs is essential; hence the need for a privately enhanced ISA SNS.

Objective: This article presented sOcialistOnline – a newly developed SNS, duly secured and platform independent with various ISA techniques fully implemented.

Method: Following a detailed literature review of the related works, the SNS was developed on the basis of Object Oriented Programming (OOP) approach, using PhP as the coding language with the MySQL database engine at the back end.

Result: This study addressed the SNS requirements of privacy, security and services, and attributed them as the basis of architectural design for sOcialistOnline. SNS users are more aware of potential risk and the possible consequences of unsecured behaviours.

Conclusion: ISA is focussed on the users who are often the greatest security risk on SNSs, regardless of technical securities implemented. Therefore SNSs are required to incorporate effective ISA into their platform and ensure users are motivated to embrace it.

Introduction

Although Google is considered the most visited website in the world (Kyle 2011; Shamim 2011), it has been competing favourably with Facebook. For instance, as of 2010, Facebook was the second biggest website in the United States of America (USA) (HuffpostTech 2011; Kiesow 2011). Since February 2011, Facebook has become the second most visited website in the average country in the world (Shamim 2011), with statistics confirming the second place position in the USA and the United Kingdom (Kyle 2011). However, as of November 2013, Facebook has been ranked as the largest media site in the entire world (Smith 2013; Vaughan-Nichols 2013).

Despite these growing economic values, which have been traced to the opportunities social networking sites (SNSs) offer to their customers in meeting friends, and even complete strangers online, many SNSs have not been able to live up to the security and privacy issues they have created (Hopper 2010:2). Specifically, Facebook has been the centre of attention multiple times resulting from issues surrounding privacy since 2010 (HuffpostTech 2011; Kiesow 2011).

Some notable SNSs have attempted, with no success, to implement technical controls to provide for their security. Accordingly, the users were more contented with the *privacy controls* of LinkedIn, until it was hacked in 2012, than with those of Facebook (Judge 2011:15). Therefore, as technical controls have failed to secure SNS in isolation, there is a need for a new SNS to be adequately secured with effective ISA techniques.

This need for a secured SNS has become more pronounced since 2012 when cyber-attacks have remained the second greatest threat in Britain after terrorism (Smith 2012). This article designs and implements a secured SNS to address security challenges in the existing SNSs using ISA techniques. The study reveals that changing human behaviour on SNSs through ISA techniques is essential and more effective.

Securing SNSs – Technical controls

Facebook has initiated architectural features that have exposed data many times, thereby making

SNS users uncomfortable (Lucas & Borisov 2008:2). The introduction of a *news feed* is a noted example in which the activities of one's friends are amassed into one page. This then confirms that privacy breaches remain feasible whether or not the users painstakingly configure their privacy settings. It is especially the case now that privacy controls have little impact on how Facebook handles its backend data but only limits information flow within the SNS interface.

Although Giles (2007:17–24) highlights some security design patterns and measures, which can be implemented and practiced by service providers to prevent possible methods attackers may follow to attack the users' information, the risk associated with architectural features has been addressed by Lucas and Borisov (2008). They make use of encryption technology to introduce a design capable of safeguarding all data coming out of Facebook. However, their architectural design swaps security for usability in order to minimise the disturbance given to the users' workflow, and at the same time it retains universal accessibility. They have come up with a prototype Facebook application that makes use of proxy cryptography to resolve major restrictions on the Facebook platform.

In spite of all the calls and agitations by vendors necessitating the importance of security products, Stephanou and Dagada (2008:3) explain that 'many critical security activities have not and cannot be automated'. This is because, as Mataracioglu and Ozkan (2010:4) emphasise, 'only a small percentage of information security is maintained by *technical security* measures, while its greater percentage depends on the user'. Organisations have invested heavily in firewalls, antivirus systems and other technologies, yet they continue to suffer from severe IS breaches, and these problems are getting worse (Gartner 2011).

Technologies that offer security continue to require effective running by people, implying that organisations cannot achieve their security desires without *people.* However, as the individual is generally considered as the weakest link in the Information Security circle (Van Niekerk & Von Solms 2004:2), it is clearly a requirement that the users are given proper training on Information Security policies. Hence, the need for effective ISA on the SNSs is emphasised.

ISA techniques

Much research has been carried out on ISA techniques but most of these techniques are not based on a theoretical model; instead, they only guide about the right methods to use (Stephanou & Dagada 2008:6). For example, the research undertaken by Heidari (2010), Hinson (2012), and Wolf (2010) all shows detailed work on the methods used to secure SNSs.

The research of Kumaraguru *et al*. (2007) prove that security awareness materials can be effective when implemented, but online materials that create user awareness about phishing threats are more effective as users tend to recognise phishing sites more accurately. They also advocate for an improvement in the quality of awareness materials, and also improved awareness techniques to enhance the users understanding of the same materials.

Johnson (2012:8), in his doctoral research work conducted at the University of Lagos in May 2012, argues that much is expected from the audience. This undermines the fact that security processes can only be effective when the audience has a good security support and appreciates the security requirements. On this basis and by applying background training, Jagatic *et al*. (2007:96) are able to prove that it is very easy (through SNS in particular) to capture huge amounts of data for effective phishing attacks. They also attempt, but with no success, to measure the influence of information relating to social context on phishing attacks. What makes their work different is that e-mails are spoofed to deceive users, as if they are from friends in the SNS and, in the end, the total number of victims to this phishing attack outweighed the expectation (Jagatic *et al*. 2007:97).

Research methodology used to develop sOcialistOnline

Dynamic Systems Design Methodology (DSDM) is used to develop the SNS in this research work. This is because, like Joint Application Development (JAD) methodology, DSDM has proved to be one of the best methods when handling a project that must be completed to tight deadlines. Goodwin (2011) explains DSDM thus:

> It is a set of specification and design notations for object-oriented systems, combining features from methods devised by three methodology gurus: Grady Booch, James Rumbaugh and Ivar Jakobsen. (n.p.)

The development of sOcialistOnline is handled by the development, security, and the user acceptance teams (UAT) headed by the author. As illustrated in Figure 1, it is based on an exploratory approach using an object oriented programming (OOP) methodology for application (SNS) development. To discourage security threats through exposure to third party applications, the use of such applications to secure the SNS is discouraged.

Designing the SNS

When planning to create the SNS, the development team followed the philosophy of Steve Jobs – 'Lesser artists borrow; great artists steal' (Duffy 2010) by integrating the steps developed by Timothy Duffy with the processes highlighted by Adams (2012) to develop and implement the sOcialistOnline. These integrated steps and procedures include crafting a concept, establishing a name, obtaining venture capital, and hiring the employees.

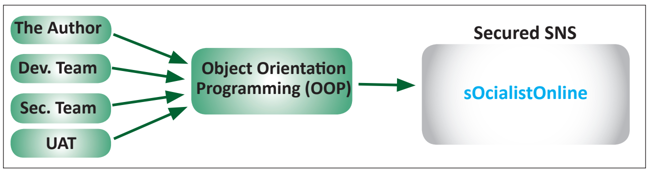

FIGURE 1: Development process for sOcialistOnline.

The Requirement

According to Aiello and Ruffo (2011:3), 'a SNS is defined, in its most general meaning, as a customisable suite of interoperable, identity-based applications'. In this context, every user composes their own combination of applicative modules, or widgets, into a customised application suite where every widget can share data with other, possibly heterogeneous, widgets running locally or remotely.

Given this general definition, there is a set of desired network requirements as well as *password file* settings and requirements that are common to so many social widgets. Such requirements classified as privacy, service, password settings, security, and ISA are applied as the basis of architectural design of the sOcialistOnline framework.

Developmental tools

The development of sOcialistOnline is based on the Object Oriented Programming (OOP) approach, using PhP as the coding language with the MySQL database engine at the back end. The programming approach, language, and database deployed are summarised as follows:

- **Programming language:** There are several web scripting languages suitable for this research work, which include ASPX (from Microsoft Inc.), PhP (from Zend coy.), JSP (from Java), and ColdFusion (of Macromedia). However, for its additional characteristics of robustness and platform independence, as discussed in section 6.9, the development team prefers to use PhP 5.3.8, the latest version as of January 2012.
- **Database:** *MySQL* works very well with PhP because it supports MySQL natively. Using MySQL for data storage, there is no need for a third party code to connect the PhP script with the database; it has already been integrated into the PhP core. For effective security, *one-way* encryption cryptography was applied using the crypt algorithm for both the username and password. This ensures that, once encrypted, the password and username table cannot be decrypted again.
- **Programming approach:** OOP is employed as the coding style, in which all the tables have their own classes. When working with a table in the database, the class of the table provides all the functionalities needed. One notable determinant feature of OOP is inheritance. Every class inherits connect functions from the Dbconfig which connects the subclass to the database. As this is a web application that is not yet supported by PhP, polymorphism could not be applied.

Technical controls on sOcialistOnline

Fundamentally, every individual is entitled to privacy, although privacy on its own is difficult to define and formalise (Aimeur, Gambs, & Ai Ho 2010:173). Millions of internet users are accustomed to spending much time on chatting, commenting, blogging, and posting photos on SNSs, and these are the activities that eventually expose them to different privacy risks. Unfortunately, most of the current SNSs do not value the principles of data minimisation and data sovereignty (Aimeur *et al*. 2010:173). Some of the technical controls implemented to secure sOcialistOnline are discussed below:

- **Customisation of access controls:** The access controls, as obtainable in the popular SNSs, on sOcialistOnline, are customised based on the users' groups and information type. Typically, a user has different classes of acquaintances including close friends, family members and colleagues at school or work. Unfortunately, only very few SNSs (such as Facebook, MySpace and Bebo) provide *privacy* settings that are elaborate where user profiles are broken into several small elements (Basic info, personal info, wall post, friends, etc.) (Aimeur *et al*. 2010). An experiment performed by Iyer (2009), and verified by Aimeur *et al*. (2010), confirms that the privacy settings on Facebook are erroneous and therefore not very effective, especially when a particular friend is to be restricted by his or her friend from accessing specific personal information. This ineffective access control exposes the user's privacy to security, reputation or credibility risk. sOcialistOnline is therefore designed in a way that the users can easily group their friends into user categories, making it possible to restrict the information type to the user group by means of a simple access control mechanism.
- **User-friendly way of setting privacy:** Unlike Facebook, the user's privacy settings on sOcialistOnline are flexible to customise, and are also integrated with a user-friendly interface that is easily understood by any typical SNS user.
- **Customised search:** A customised search is implemented on sOcialistOnline to further enhance the preservation of the user's privacy. It is therefore possible for a user to specify an individual who can search his or her profile, and the information types that can be searched. A screen-print of a customised search on sOcialistOnline is displayed in Figure 2.

For instance, a user may choose to ensure *unobservability* (that is, not be noticeable as a registered user on an SNS) and may want to remain totally invisible to those who are not in his or her list of friends. A user can also classify his or her personal data as 'sensitive' or 'not sensitive' relative to the search process. For example, a user may be indifferent to another user finding his or her name and sport of interest but not for

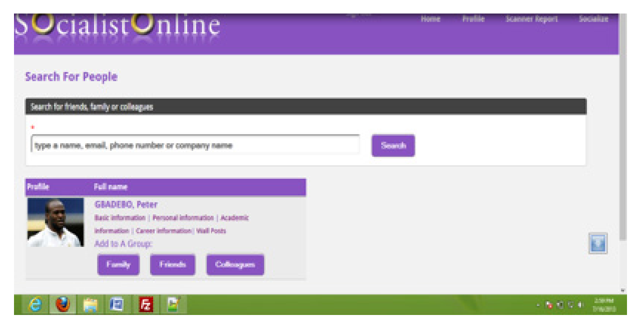
sOcialistOnline
Home
Profile
Scanner Report
Socialize
Search For People
Search for friends, family or colleagues
type a name, email, phone number or company name
Search
Profile
Full name
GBADEBO, Peter
Basic information | Personal information | Academic information | Career information | Wall Posts
Add to A Group:
Family
Friends
Colleagues

FIGURE 2: Screenshot for customised search.

sensitive information such as religion:

- **Active blocking of information related to users:** In addition to *customisation search,* which is implemented for a user to specify his or her profile information that could be searched, the sOcialistOnline offers the facility for a user to untag objects from his or her profile. Hence, an individual may consider a particular photo too sensitive and therefore choose to remove the link from his or her profile and, thus, mitigate the potential risk of the picture appearing when his or her identity is searched.

ISA techniques

Several authors such as Brodie (2009), ENISA (2007), PriceWaterHouseCoopers (2010), and Hinson (2012) have established that an SNS cannot be adequately secured without effective ISA. Hence, the author implemented the following ISA techniques into the sOcialistOnline to further enhance its security and user privacy:

- **Explicit privacy policy:** Generally, SNSs have a privacy policy but they often implement this to emphasise the significance of the users' privacy to the network and not to the users *per se*. Therefore, in most evaluations regarding the users awareness to the privacy policy, less than 10% of SNS users claim to have read and understood the policy document of their SNS (Jones & Soltren 2012:3). This is partly attributed to the fact that the document is always too long, with an average mean length of 2633 words and a median of 2.245 (Bonneau & Preibusch 2009:254). The same situations apply to the terms and conditions. sOcialistOnline addresses this situation by summarising the policy statements into three pages, and applies the *terms and conditions* as a multiple alternative option. In which case, rather than the usual *terms and conditions*, a user-friendly community guideline is published on the sOcialistOnline to educate users in *real-time*.
- **Privacy awareness and customisation:** The sOcialistOnline is flexible enough for users to express their data as a privacy policy, and makes it possible for them to automatically compare the compatibility of the privacy response of the users to that of the SNS. This is what *the terms and conditions* entail. Where there is incompatibility, a user is warned and notified instantly, although he or she may still continue with the registration. This awareness function also alerts the user of his or her unsecured privacy settings each time he or she logs on to raise his or her ISA.
- **Data minimisation:** As only the information required should be disclosed in all instances, SNS users should be able to confirm the information type that is accessible to the SNS services (providers and third party applications), and their use. SNSs should also clarify the user's personal data of interest to them, and state clearly what exactly their interest is concerned with for the data owner to decide whether or not to accept or reject the SNS services. An in-built mechanism is incorporated into the sOcialistOnline to restrict access to user information and authorised data only (Aimeur *et al*. 2010:176).
- **Privacy lens:** It is required of an SNS user to view his or her profile the exact way it will appear to others, for him or her to appreciate that his or her data are unsecured. This is exactly what the privacy lens is all about and it is targeted at raising the user's information security awareness on sOcialistOnline (Aimeur *et al*. 2010:175).
- **Password standardisation:** To guide against guessable password formulation, the sOcialistOnline incorporates Persuasive Text Password (PTP), as proposed by Forget *et al*. (2008), whereby the system auto-generates some characters and inserts them into a users' password combination. The PTP plays a middle-man role between a system generated password, which is always strong but difficult to remember, and one that is user-generated that is often weak but easily remembered. However, the sOcialistOnline makes it highly flexible and optional for SNS users to accept, reject or even request alternative characters and numbers at will.
- **Password monitoring:** In line with the user's consent, the sOcialistOnline generates and keeps personal and confidential data, including the user's passwords and photographs. This is the main input data for this research work. The development team included a *password scanner*, which scans the password, files and analyses the strength of the individual password. This solution prompts each user, at every log-on, to *inform* him or her about the strength of his or her password and advise the user to reset it accordingly, but continues to allow the user to proceed at his or her own risk. This alert pops up at the registration stage and also at every user login to eliminate the user's acclaimed ignorance of ISA, and to ensure that every individual is fully aware of the potential risk.

System testing, security and publicity

This section addresses the processes wherein the sOcialistOnline was tested, and checked to verify if it is technically secured and published for general use.

Unit and UAT testing

Available Software Development Life Cycle (SDLC) testing scripts were used to unit test the SNS. A UAT script designed by the development team was reviewed by the ICT directorate, of Tai Solarin University of Education (TASUED), Nigeria, before being presented to the testing, comprised of members of the student affairs directorate and the students' union executives. To maintain his independence, the author was not involved in the actual UAT exercise. Instead, the testing was supervised by a system analyst at the university's e-learning centre and implemented by only seven students and three non-academic staff, all of whom are knowledgeable about SNS. Informed consent forms were completed by each of the testers stating that participation was free and optional. The testers were satisfied with the sOcialistOnline, although they came up with some comments that have nothing to do with the system functionality but with the speed, stability and availability of the SNS. These problems were addressed immediately as they were problems caused by the internet service provider (ISP) who hosted the SNS server.

System security

As a result of the increasing rate at which SNSs are being attacked, Summit Technology Nig. Limited was employed to tighten up the web and application security. The focus was mostly on operating systems and the Internet Explorer platforms where the sOcialistOnline is hosted, to ensure that certain services are working correctly and securely, as they should be.

System publicity

Usually SNSs are known to experience low patronage when they are newly implemented (Khan et al. 2011). To stop or reduce this fear, the author increased user awareness amongst the university students and staff by employing the Student Affairs unit and the Staff Union government of TASUED to encourage their members to patronise the site.

Some students were invited to a presentation session on the SNSs. The author issued the invitation to some students and staff but made it clear that the participation was free, optional and anonymous. This seminar included a short question and answer session where participants were free to express their concerns about the project. The participants were also given adequate ISA guidelines towards their behaviour on SNSs in general, but with emphasis on sOcialistOnline. The seminar was organised a few days after the SNS was implemented and in the production environment, in order to promote its publicity and awareness amongst the audience and other intended users.

Results

This article discusses the development and implementation of the sOcialistOnline site. This SNS was secured by technical and ISA techniques before being migrated to the internet. Similarly, the UAT and system testing were performed but these are limited to the postulated model, and the conclusion is based on the evaluation of data obtained. Different types of technical controls, which form part of the body of a secured SNS, are evaluated with special emphasis on the incorporated ISA techniques.

Although a secured SNS is ultimately designed and implemented, the emphasis of this article is on the ISA techniques used to secure the SNS, because they are the main distinguishing factors from the existing ones.

Conclusions and recommendations

The sOcialistOnline is developed and secured by the technical and ISA techniques before being migrated to the production environment. Similarly, the UAT and system testing were performed but are limited to the postulated model and the conclusion is based on the evaluation of the data obtained. Different types of technical controls, which form part of the body of a secured SNS, were evaluated with special emphasis on the incorporated ISA techniques. The SNS is therefore adjudged to be better secured when compared to these inadequate ISA techniques. Notwithstanding this, the *effectiveness* of these controls and techniques proposed and implemented will be subjected to absolute measurements using a non-incident statistic approach, as this is an on-going study.

It is recommended that SNSs should emulate the ISA efforts implemented in this study, and much more if possible, to raise the users' awareness maximally. Moreover, the *terms and conditions*, and the user-friendly community guidelines, should always be published on the sites to educate the users in real-time. Accessible and polite languages are also required to enhance the users' understanding and compliance with the SNS's regulations.

Acknowledgements

This scientific article is one of the final products of my research carried out during my (Julius O. Okesola) PhD study at the School of Computing, University of South Africa (UNISA). Some other final products have been published in other recognised journals.

I therefore acknowledge, with thanks, Prof. Segun Awonusi (the Vice Chancellor of TASUED) for giving me the inspiration; Abiola Okesola (my wife) for her quiet wisdom and unfailing loyalty; and, more importantly, Prof. Marthie Grobler – my project supervisor – for her foresight in identifying values, shortcomings and obstacles; her aptitude for putting an idea into context; and above everything, for being patient and understanding.

Competing interests

The authors declare that they have no financial or personal relationship(s) that may have inappropriately influenced them when they wrote this article.

Authors' contributions

J.O.O. (University of South Africa) was the lead author of this article. The contribution of M.G. (University of South Africa) was in the capacity of co-author.

References

Adams, 2012, 'Creating a social networking site like Facebook', *Advanced PHP Solution*, viewed 09 June 2013, from http://advancedphpsolutions.com/blog/social-networking/create-a-social-networking-site-like-facebook

Aiello, L.M & Ruffo, G., 2011, 'Tunable privacy for distributed online social network services', *Computer Communication*.

Aimeur, E., Gambs, S. & Ai Ho, 2010, 'Towards a privacy-enhanced social networking site', *2010 International Conference on Availability, Reliability and Security*, viewed 07 June 2011, from http://www.mendeley.com/research/towards-privacyenhanced-social-networking-site-17

Bonneau, J. & Preibusch, S., 2009, 'The privacy jungle: On the market for data protection in social networks', *The Eighth Workshop on the Economics of Information Security*, (WEIS 2009), Greece, pp. 250–261, viewed on 14 June 2014, from http://weis09.infosecon.net/files/156/index.html

Brodie, C., 2009, 'The importance of security awareness training', in *SANS Infosec Reading Room*, viewed 23 May 2011, from http://www.sans.org/reading_room/whitepapers/awareness/importance-security-awareness-training_33013

Duffy, T., 2010, Nine steps to creating a social networking site that kills Facebook, *TECHi.com*, viewed 09 February 2013, from http://www.techi.com/2010/06/9-steps-to-creating-a-social-networking-site-that-kills-facebook

ENISA, 2007, 'Information Security Awareness Initiatives: Current Practice and Measurement of Success', viewed 18 May 2011, from http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/enisa_measuring_awareness_final.pdf

Forget, A., Chiasson, S., Van Oorschot, P. & Biddle, R., 2008, 'Improving text passwords through persuasion', *4th Symposium on Usable Privacy and Security* (*SOUPS'08*), June 2008, Pittsburgh. http://dx.doi.org/10.1145/1408664.1408666

Gartner, 2011, 'User awareness in social networking', viewed 01 June 2012, from http://www.Gartner.Com/Research/Spotlight/Asset_118887_895.Jsp

Giles, H., 2007, 'Security Issues and Recommendations for Online Social Networks', in *ENISA Position Paper #1*, viewed 2 May 2011, from http://www.ENISA.europa.eu/act/res/ other-areas/social-networks/security-issues-and -recommendations-for-online-social-networks

Goodwin, C., 2011, Development technology in under 10 minutes, *ComputerWeekly.com*, viewed 12 June 2014, from http://www.computerweekly.com/feature/Development-methodology-in-under-10-minutes

Heidari, H., 2010, 'Design patterns and refactoring for security in social networking applications', in *Multimedia University, Malaysia*, viewed 15 December 2011, from http://www.kaspersky.com/se-asia-it-security-conference

Hinson, G., 2012, 'The true value of IS awareness', *Noticebored,* viewed 23 August 2011, from http://www.noticebored.com/html/why_awareness_.html

Hopper, E., 2010, 'Intelligent strategies and techniques for effective cyber security, infrastructure protection and privacy', *The 5th International Conference for Internet Technology and Secured Transactions (ICITST-2010)*, London, UK, 8–10 November.

HuffpostTech, 2011, Facebook tops Google as most visited website of the year, viewed 23 July 2011, from http://www.huffingtonpost.com/2010/12/30/facebook-tops-google-as-m_n_802606.html

Iyer, A., 2009, 'Are Facebook's privacy settings working?', viewed 03 February 2012, from http://www.artificialignorance.net/blog/facebook/arefacebooks-privacy-settings-working

Jagatic, T.N., Johnson, M., Jakobsson, M. & Menczer, F., 2007, 'Social phishing', *Communications of the ACM* 50(10), 94–100. http://dx.doi.org/10.1145/1290958.1290968

Johnson, A., 2012, 'Social network settings are ineffective', *Information and Communication Journal* 12(3), 8.

Jones, H. & Soltren, J.H., 2012, 'Facebook: Threats to privacy', *Project MAC: MIT Project on Mathematics and Computing.*

Judge, P., 2011, 'Social networking security and privacy study', *Barracusalabs Networks Inc.*, viewed 03 February 2012, from http://www.Barracudalabs.Com/Snsreport/2011socialnetworkingstudy.Pdf

Kiesow, D., 2011. Facebook, most visited website of 2010, valued at $50 billion, *Poynter*, viewed 23 July 2011, from http://www.poynter.org/latest-news/media-lab/social-media/112651/facebook-most-visited-website-of-2010-valued-at-50-billion/

Khan, B., Alghathbar, K.S., Nabi, S.I. & Khan, M.K., 2011, 'Effectiveness of information security awareness methods based on psychological theories', *African Journal of Business Management* 5(26), 10862–10868.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L., Hong, J. & Nunge, E., 2007, 'Protecting people from phishing: The design and evaluation of an embedded training e-mail system', *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, San Jose, California, United States of America, pp. 905–914. http://dx.doi.org/10.1145/1240624.1240760

Kyle, A.H., 2011. Top 10 most visited website of 2011, *Kaleazy Creative*, viewed 23 July 2011, from http://Kaleazy.com/top-10-most-visited-websites-of-2011

Lucas, M. & Borisov, N., 2008, 'Flybynight: Mitigating the privacy risks of social networking', *Proceedings of the 7th ACM Workshop on Privacy in the Electronic Society*, ACM New York, New York, United States of America, pp. 1–8.

Mataracioglu, T. & Ozkan, S., 2010, 'User Awareness Measurement through Social Engineering', *International Journal of Managing Value and Supply Chains* 1(2), 27–34.

PriceWaterHouseCoopers, 2010, 'Protecting your business – security awareness: Turning your people into your first line of defence', viewed 25 July 2011, from http://www.pwc.co.uk/eng/publications/protecting_your_business_security_awareness.html

Smith, E., 2012. 'The true cost of cyber-security – Why your company should invest in it', *Enlight Research*, viewed 01 August 2013, from http://www.enlightresearch.com/ideas/2012/7/9/the-true-cost-of-cyber-security-why-your-company-should-inve.html

Smith, C., 2013, 'The planet's 24 largest social media sites, and where their next wave of growth will come from', *Business Insider,* viewed 09 December 2013, from http://www.businessinsider.com/a-global-social-media-census-2013-10

Shamim, S., 2011, 'Top 10 most visited websites in the world', *Expert Review now,* viewed 25 July 2011, from http://www.expertreviewnow.com/2011/02/top-10-most-visited-websites-in-the-world/

Stephanou, A.T. & Dagada, R., 2008, 'The impact of ISA training on IS behaviour: The case for further research', *Proceedings of the Information Security for South Africa - ISSA 2008: Innovative Minds*, School of Tourism and hospitality, University of Johannesburg, South Africa, pp. 311–330, viewed 28 August 2012, from http://if08030.files.wordpress.com/2011/06/issa2008proceedings.pdf

Van Niekerk, J. & Von Solms, R., 2004, Organizational learning models for information security education', *A Proceeding of ISSA*, Johannesburg, South Africa.

Vaughan-Nichols, S.J., 2013, 'Facebook remains top social network, Google+, YouTube battle for second', in *ZDNet,* viewed 09 December 2013, from http://www.zdnet.com/facebook-remains-top-social-network-google-youtube-battle-for-second-7000015303/

Wolf, M.J., 2010, 'Measuring ISA programme', Master's thesis, Department of Information Systems and Quantitative Analysis, University of Nebraska, Omaha.