Proceedings of the 7th World Conference on Information Security Education
9-10 June 2011, Lucerne, Switzerland

Towards Information Security Education 3.0
A Call for Information Security Educational Ontologies

Johan Van Niekerk and Ryan Goss

Institute for ICT Advancement, Nelson Mandela Metropolitan University
johan.vanniekerk@nmmu.ac.za, ryan.goss@nmmu.ac.za

Abstract. The need for information security "know-how" has permeated to all aspects of modern society. Nowadays, information security is no longer a problem faced by organizational users alone. Individuals often use online services in cyberspace on a daily basis for activities ranging from personal banking to social networking. The need to educate users regarding secure behavior in cyberspace has subsequently also become well established. This paper firstly argues that approaches towards such "cyber-security" education should be based on the same Web 2.0 philosophies and paradigms that made the use of the Web in daily life so popular. Finally the paper briefly discusses the need for future research to enable such an approach towards information security education.

1 Introduction

The advent of the Internet has brought many advantages to humanity. For the first time in history humans are able to communicate and collaborate in almost real-time, with ease, virtually irrespective of national borders and/or time zones. In recent years information technology has become such an intrinsic part of modern business that some authors no longer see the use of information technology as a strategic benefit. Instead, it can be argued that information technology is a basic commodity, similar to electricity, and that the lack of this commodity makes it impossible to conduct business [1].

However, the benefits of information technology and the Internet do not only apply to organizations. Increasingly, the Internet is being used as a tool for personal business, entertainment, communication, and many other activities by individuals at home. Online activities are also not restricted to only the rich, or the educated, or any other specific demographical grouping. According to the World Bank (2010) 8.6% of all South Africans was Internet users in 2008. Amongst urban South Africans this figure is substantially higher. Kreutzer [2] found that 83% of low-income black South African youth in an urban township uses the Internet via mobile phone technology on a typical day. Even amongst school children the use of online technologies and/or platforms has become almost ubiquitous due to the low cost of access using platforms like, e.g. MXit. It can be argued that the Internet, in one form or other, today is being used by all demographic groups, including the young and old, rich and poor, educated and uneducated, urban and rural.

Unfortunately, the Internet has not only brought advantages. It has also brought numerous new risks. In an organizational context, typically these risks can be mitigated through the use of various information security controls. For organizations these controls are usually selected with the aid of internationally accepted standards such as ISO/IEC 27002 and ISO/IECTR 13335-1. These information security controls, to a large extent, depends on the actions of organizational users in order to work correctly. Humans, at various levels in the organization, play a vital role in the processes that secure organizational information resources. Many of the problems experienced in information security can be directly contributed to the humans involved in the process. Employees, either intentionally or through negligence, often due to a lack of knowledge, can be seen as the greatest threat to information security [3, p. 3]. Organizations typically address this lack of information security related knowledge through formal information security awareness and educational programs. Many current research publications focus on organizational information security education and many companies specialize in providing such education as a service. Unfortunately, almost no-one currently provides equivalent information security education for individuals using the Internet in their personal capacities.

The need for information security education outside the corporate environment has become widely recognized. Furnell [4] likens the Internet to a jungle, with uneducated users falling "prey" to online "predators". Siponen [5] identifies the need for five "dimensions" of information security awareness education, one of which is the "general public" dimension. Siponen [5] also argues that society as a whole has an ethical responsibility to ensure that its vulnerable groups receive appropriate information security education. As an example; South Africans in general have a well-developed culture of personal security. Most South Africans are used to assessing the risks posed by "normal" day-to-day activities and also know how to mitigate such risks, e.g. through locking the doors at night, avoiding walking through dark alleys, not leaving personal possessions unattended, etc. However, due to the relative newness of Internet access for many citizens a *culture of cyber-security* is still lacking.

Many South Africans, especially from vulnerable groups, such as the elderly, are completely unaware of even the existence of many risks during "normal" online activities and thus can easily fall prey to online "predators". During 2010 alone approximately 4400 cases of identity theft, involving losses of more than R200 million, have been reported to the SAFPS (www.safps.org.za). As the so called "digital divide" is reduced, progressively more South Africans will be put at risk of having their identities stolen. The only way to effectively mitigate this, and other risks posed by Internet access, is through increased awareness of the risks posed by this medium, and education regarding how these risks can be mitigated.

There is a need for information security education for all "cyber-citizens". Furthermore, due to the diverse backgrounds, educational levels and many other factors of the various vulnerable groups, a "one size fits all" approach to such education cannot work. It can thus be argued that information security educa-

tional programs would have to be tailored to the specific needs of each target user group in order for such programs to be effective. The aim of this paper is to argue that there is a need for a freely accessible "cyber-security portal" through which any Web user can access relevant information security educational programs. Furthermore, the paper briefly explores the idea of basing such a portal on a Web 2.0, and hence E-learning 2.0, paradigm and then presents a call for further research towards such educational approaches.

2 Why E-learning 2.0?

The rapid advancement, and global acceptance, of the Internet and World Wide Web has left modern society in general somewhat unprepared for the digital economy we now live, and work, in. In the past the general spread and use of major technological advancements happened at a pace that still allowed society to gradually develop ways of dealing with it. The widespread use of the automobile, for example, happened over more than one generation. This allowed people time to develop ways and means of acting safely in and around cars. This behavior was then passed from one generation to the next allowing the development of a "culture" where all members of society are aware of the dangers motorized vehicles could pose to their personal safety. The rate at which use of the Web penetrated society did not allow the formation of such a "culture". Not only are we still in the first generation of web-users, but the technology used is still changing rapidly.

One of the best examples of the rapid acceptance of new technology in modern society is the recent advent of social networking and other Web 2.0 phenomena. The participatory, collaborative, and dynamic online approach of Web 2.0 is arguably where most serious efforts at Web-based development are currently heading; therefore, it follows that online learning communities would naturally transform to use a similar approach [6]. By following the trends of Internet users, these new learning environments prepare the learner for operating in the real world. While it is true that some aspects and characteristics of the current educational system will most likely prove resilient as the preferred method for learning certain topics [6], it is very likely that Web 2.0 trends will penetrate more of the educational system than one can now imagine.

Web 2.0 provides the learning environment with the tools necessary to enable learners to build their own knowledge constructs and not conform to the generic constructs of information that, for example, traditional education imposes on them. By allowing learners to construct their own knowledge and storing it in a way that is most efficient and effective for their own learning style, educators ensure the best possible outcome to the learning experience. The combination of Web 2.0 and e-Learning methodologies brings forth a new breed of e-Learning systems, known as e-Learning 2.0.

E-Learning has been suggested as a tool which could make education and lifelong learning more effective and efficient. The content driving such systems, however, is often static in nature and many of the e-Learning systems fail in

that they simply imitate previous educational paradigms [7]. This is also true of many IT-based fields as IT itself changes so rapidly with new technological advancements being introduced on a nearly daily basis. Growth of social software on the Internet and the **movement towards open educational content** has had researchers rethink previous models of e-Learning. The term "E-Learning 2.0" was coined in 2005 to describe e-Learning systems, built on social networking software (Web 2.0) and published online [8]. This e-Learning system is a new style of learning deeply rooted within the social constructivist paradigm [9], described as a revolution, converting the Web as a medium, as it is widely known and accepted, into a platform for delivery of data [8].**Content is no longer only delivered to learners, but also authored by learners**. Web 2.0 in the educational environment is considered by several authors as progressive and the driver of educational change which offers new perspectives and challenges to education at all levels.

Some of the features which make Web 2.0 so favourable to the educational sector are its **ease of publication**, **sharing of ideas** and **re-use of study content**. Commentaries and links to relevant resources in information environments that are managed by the teachers and learners themselves also make Web 2.0 favourable in the eyes of educators [7]. The idea of allowing learners the ability to manage and contribute to their learning environment is in contrast to previous education systems, where developers of the system employed creators of study content, who were tasked with building a generic knowledge base from which learners were educated. Forcing all learners to learn in the same way from such a knowledge store is not necessarily the most effective learning approach. It could be argued that Web 2.0 based systems might have more success. Previous information security education systems relied heavily on the use of formal learning techniques, whereas Web 2.0 based tools would allow learners to branch out and explore "informal" learning.

80% to 90% of all learning has been attributed to learning occurring informally outside of the classroom [10]. Informal explanations dominate over formal mathematical proofs and examples of computer applications security were found to be especially well received by learners in information security education [11]. Informal learning design is nothing new, but is something e-Learning designers have previously ignored [10]. The statistics themselves should be enough to force e-Learning design practises to incorporate more informal learning techniques [10]; however, nothing significant has to date been done about it. The possibility of implementing such a system for information security education should thus be investigated in order to ascertain its usefulness in educating all users of computer systems, world-wide.

As argued earlier, the use of computer systems has expanded from typically adults within an organization to include people from all walks of life. It has therefore become necessary for information security education to evolve beyond organizational information security towards **cyber-security education** targeting all of these would-be victims. It can be argued that E-Learning 2.0 systems are ideally suited to this task, as they are built on the Web as a platform, and

uses technologies already reaching these would-be learners during other activities. Furthermore, e-Learning 2.0 systems allow the user to act as both a consumer and a producer, allowing them to "Rip, Mix and Feed" [10]. This process allows for the education content created to be authored by many individuals, instead of being tasked to a single person or team. This means that the creation of the information security education content base becomes a community endevour, *which requires various rating systems to be implemented in order to decern the credibility of the authors and the works which are produced as a result of such a community endevour*. By allowing learners to not only draw from, but also contribute to the content base, the learner is assured a sense of ownership for the content they produced. Providing a sense of ownership creates an appetite for further learning, the learners within a system are thus **motivated** to continue their education and further themselves. This motivation stems from the system actively engaging the learner in the learning process, by requiring them to integrate and maintain the social software tools which allow the learning to happen [12].

The advantages of e-Learning 2.0 systems are extensive and elaborate, allowing these systems to fast become viable options for replacing many of the traditional learning systems in production today. It is thus the assertion of this paper that the use of E-learning 2.0 for "cyber-security education" could be the ideal way to address the growing need to educate learners from all walks of life, enabling them to be "safe" whilst online. Unfortunately, the advantages offered by such "revolutionary" education technology are also accompanied by certain challenges which could hamper the development and success of such systems. The most notable of these challenges will be briefly examined in the next section.

3 Problems with learner-generated learning material

The promotion of learner-assisted content publishing and creation allows an abundance of information on a number of cyber-security related topics to be generated. The generation of such volumes of information produces yet another potential problem. Firstly, instead of a *lack* of sufficient information security content, learners could potentially suffer from *information overload* [13]. One of the problems with traditional e-Learning systems was that it took a long time and a lot of financing in order to build a suitable knowledge base from which to educate learners. Developers of the coursework of information security education systems are typically experts in the field developing content as part of their jobs. E-Learning 2.0 allows the learners themselves to contribute and build up the learning material, building a system based on "folksonomy" or user-generated taxonomy. Although this can provide many advantages, it also gives rise to the potential for **information overload**. If learners are not limited to the scope of a contribution, certain information security topics may have a large amount of content associated with them, so when a learner searches for a particular topic, too much information is returned and the learner is unable

to manage and sift through it to find specifics [13]. Secondly, in order to ensure wide acceptance of learner generated content, a mechanism to ensure the validity of such content would be needed. The integrity of the information available at sources such as wikipedia is often questioned precisely because of the lack of such mechanisms. Critics of learner-created content in general express concerns about trust, reliability and believability of such content [14].

Any proposed system must allow the large amount of information posted to be managed in an effective way, so that learner searches are optimized and only information pertinent to a specific search are returned. This is currently still difficult to accomplish on e-Learning 2.0 systems, as each typically provides its own proprietary knowledge storage facility, each differing in design from other such applications. This means that for one system to share content with another system, it would need to provide an API to its knowledge store and the receiving application would need to write specific code in order to interact with this API. This type of code would need to be written for all remote knowledge stores that the receiving application wishes to interact with, severely limiting the scope of applications which can interact with one another. One possible solution to this problem that is currently being developed and is fast gaining momentum as the next wave in the evolution of the Web, is the Semantic Web.

4 Towards Information Security Education 3.0

Web 2.0 opened the Web and allowed contribution of information by the average computer user. This contribution facility, although solving the problem of content generation, introduced further problems which needed to be addressed in order to ensure the continued success of the Web and facilitate its large growth. One of the problems with allowing contribution from many sources, is that of information overload. The information posted is generally stored in a format suitable only to human readers, making it very difficult for machine users (or applications) to understand and draw inference from it. This meant that machine users and applications are unable to understand information security concepts and the contributions learners make on the system. **Although information security education concepts would be *machine readable*, they would not necessarily be *machine understandable*** [15]. In order to facilitate searches which filtered through all of this information accurately and effectively, preventing information overload to the users of the system, machine users need to be able to parse the information and have an understanding of its contents.

The Semantic Web can be thought of as a large relational database, joining tagged items and incorporating all topics and concepts, from book chapters to cell phones to the price of laptop computers [13]. By joining these topics in a way which computer applications can understand, the Semantic Web allows information generated by learners on an information security education system to be transformed from a "display only" form, only parsable by humans or software agents written specifically for the task, to a vast database of knowledge, which **computer applications can parse and understand** [13]. This knowledge

allows computers to more accurately search for specific criteria within the information security education system content base and do much of the grunt work in information processing and filtering for searches performed by human users of the system. The Semantic Web further allows users to find relationships between tagged items, such as related information security topics [13]. This process is possible due to the Semantic Web's ability to use inference rules and data organizational tools known as "ontologies", which are domain theories, enabling a Web that provides a qualitatively new level of service [13] [15].

An ontology, according to Gruber 2003 is a formal and explicit specification of a shared conceptualization [16]. Formal, meaning it should be represented in a formal representation language and shared, indicating that the ontology describes knowledge accepted by a community [16]. A primary goal of ontologies is to facilitate knowledge sharing and reuse, providing a common understanding of various content that reaches across people and applications on the Semantic Web [15]. The only way learning systems on the Web which share domain and pedagogical knowledge amongst themselves will work is if a large number of ontologies surrounding these systems exist [15]. Currently, this is not the case as there are few domain ontologies in existence and even fewer which cover instructional design and learning theories [15]. For this reason, the learning community in general, and in this case the information security educational community specifically, needs to come together and develop the standard ontologies in a collaborative way, much like the contributions to a wiki, where all users input is valued, condensed and refined by the community working toward a common goal.

One of the main reasons for the lack of such standardized ontologies for learning is the apparent lack of standard vocabulary in the domain of education and instructional design [15]. Many standards groups are in the process of addressing these and other issues. However, no current group are dedicated to the creation of information security educational ontologies.

5 Conclusion

There is a need for information security education beyond the confines of modern organizations. Individuals from all walks of life are using the Internet as a tool for personal business, entertainment, communication, and many other activities. These individuals need to be educated in order to help protect them from the dangers posed by engaging in such activities online. Such education should be in a form that encourage people to engage in it on a voluntary basis. One possibility to explore is the leveraging of the Web 2.0 philosophy in order to engage such learners in the participatory creation of learning content. The idea of such an e-learning 2.0 approach has been suggested by several educational researchers but its effectiveness has yet to be proved. However, before such an approach could become a reality subject specific ontologies for the intended subject matter would be needed. The authors of this paper wish to call on the fraternity

of information security education researchers to start exploring the possibilities offered by Web 2.0, e-learning 2.0 and Semantic Web technologies. Furthermore this paper wishes to call on these, and future, researchers to collaborate, and contribute, towards the needed shared information security educational ontologies needed to make Information Security Education 3.0 a reality. It is thus not the intention of this paper to present completed research, but rather to serve as a catalyst for future research.

References

[1] Carr, N.G.: IT Doesn't Matter. Harvard Business Review (2003) 41–49
[2] Kreutzer, T.: Internet and online media usage on mobile phones among low-income urban youth in cape town. Mobile 2.0: Beyond Voice? Pre-conference workshop at the International Communication Association (ICA) Conference Chicago, Illinois, 20 21 May 2009 (2009)
[3] Mitnick, K., Simon, W.: The art of deception: Controlling the human element of security. Wiley Publishing (2002)
[4] Furnell, S.: Its a jungle out there: Predators, prey and protection in the online wilderness. Computer Fraud & Security (October 2008) 3–6
[5] Siponen, M.: Five dimensions of information security awareness. Computers and Society, June 2001 (2001) 24–29
[6] Rogers, P., Liddle, S., Chan, P., Doxey, A., Isom, B.: Teaching social software with social software. Turkish Online Journal of Distance Education. ISSN 1302-6488 **8**(3) (2007)
[7] Geser, G.: Open educational practices and resources. [WWW document]. URL http://www.olcos.org/, Sited 27 September 2008. (2007)
[8] Downes, S.: E-learning 2.0. [WWW document]. URL http://www.elearnmag.org/subpage.cfm?section=articles&article=29-1, Sited 25 May 2008. (2005)
[9] Servitium: Web and learning 2.0: A servitium whitepaper. Servitium White Paper (2008)
[10] Schlenker, B.: What is e-learning 2.0? Learning Solutions, Practical Applications of Technology for Learning, e-magazine (2008)
[11] Yurcik, W., Doss, D.: Different approaches in the teaching of information systems security. Information Systems Education Conference (ISECON), Cincinnati, OH, 2001 (2001)
[12] Mejias, U.: Teaching social software with social software. Innovate: Journal of Online Education **2**(5) (2008)
[13] Ohler, J.: Web 3.0 - the semantic web cometh. University of Alaska (2008)
[14] Mason, R., Rennie, F.: Using web 2.0 for learning in the community. Internet and Higher Education **10** (2007) 196–203
[15] Devedzic, V.: Education and the semantic web. International Journal of Artificial Intelligence in Education **14** (2004) 39–65
[16] Gladun, A., Rogushina, J., Garcia-Sanchez, F., Martinez-Bejar, R., Fernandez-Breis, J.: An application of intelligent techniques and semantic web technologies in e-learning environments. Expert Systems with Applications **36** (2009) 1922–1931