

Chapter 8

Information Security Awareness in Academia

Peter Korovessis

Peter Korovessis, University of Plymouth, UK & The American College of Greece-DEREE, Greece

ABSTRACT

Information security has become an established discipline as more and more businesses realize its value. Many surveys have indicated the importance of protecting valuable information and an important aspect that must be addressed in this regard is information security awareness. The academic sector is one that regularly addresses information security awareness. Because many successful security intrusions are the result of either social engineering or user complacency, there is a need for students in non IT-related disciplines to become as security literate as possible. The proposed research investigates the level of security awareness amongst the online population. For this reason sample data from a university environment was used in order to examine the state of information security awareness in the academic sector and investigate the awareness needs of students. Since information technology grows at a rapid pace, it is important for the academic sector to identify new trends and developments in information security and adapt the curricula appropriately.

INTRODUCTION

One of the major challenges of managing an information system and its resources is to provide appropriate measures to protect these systems. Information security has become an established discipline as more and more businesses realize its value. Many surveys have indicated the importance of protecting valuable information and an important aspect that must be addressed

in this regard is information security awareness. Information security awareness is about enabling all participants in the information security function to clearly understand the role they play and are aware of the rules and regulations they are expected to adhere to.

Recent research indicates that life has become more interconnected than ever. As reported by the Pew Internet and American Life Project (Kennedy et al., 2008) the traditional American

DOI: 10.4018/978-1-4666-4157-0.ch008

nuclear family now have the highest concentration of interconnected gadgets and devices. A similar situation exists in the UK and Europe (Staksrud et al., 2007) where children are growing up with Web 2.0 and the interactive web while, on the other hand, adults are still struggling to understand and incorporate their use in their lives. At the same time, the volume and nature of information security threats have evolved targeting mainly the weakest link, which is the end-user (Schneider, 2000; Hinde, 2004; ENISA, 2008). It is understood that good security cannot be achieved by technical means alone. Online users, in order to protect themselves, must have a solid understanding of the required security measures (Shuhaili et al., 2010).

There are several sectors where information security awareness has received increased attention, namely government, industry and academia (Bishop, 2000; Yasinsac, 2002). The academic sector is one that regularly addresses information security awareness. This sector consists of academic institutions (colleges, universities, technical schools, schools of secondary education or high schools, etc.), that belong to public or private education, and have as their primary aim to provide learners with all the necessary skills and knowledge for their future occupations. These may include information security as their primary or secondary focus. The role of academic institutions in information protection is vital and has received a lot of attention from researchers worldwide (Williams, 2004). Since the use of information technology is an essential requirement for all university students, the information security curriculum must be designed to support the needs of students undertaking non-IT courses who are interested in learning how to protect their information assets and resources (Hentea et al., 2006). There are a lot of non-computing disciplines that are closely related with the protection of information (Bishop et al., 2005). Because many successful security intrusions are the result of either social engineering or user complacency, there is a need for students in non IT-related

disciplines to become as security literate as possible. Therefore, it is important to investigate the potential of raising security awareness within the existing education systems.

As a first step towards this goal, the proposed research investigates the level of security awareness amongst the online population. For this reason sample data from a university environment was used in order to examine the state of information security awareness in the academic sector and investigate the awareness needs of students in order to (1) support them during their time of study, (2) prepare them for the workplace, and (3) protect them in their wider personal use of IT systems. The paper starts with a background section that reviews current activity in the information security awareness domain and public awareness initiatives. Then the survey results are presented and interpreted using the following sub-sections: (1) background information, (2) use of IT and the Internet, (3) security knowledge and perceptions, and (4) security practices and behaviors. The paper completes with a discussion and conclusion section.

Since information technology grows at a rapid pace, it is important for the academic sector to identify new trends and developments in information security and adapt the curricula appropriately. There is a need to integrate security awareness into education. As a first step towards this process, it is important to investigate the level of awareness amongst the online population. This will ensure that learners are kept up to date with new developments and trends in information security.

CURRENT ACTIVITY AT THE INFORMATION SECURITY AWARENESS DOMAIN

The importance of information security awareness and training in order to secure critical organizational or personal information resources has been raised by many organizations.

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/information-security-awareness-academia/76597

Related Content

Theory of Critical Total History of Civilization

Andrew Targowski (2009). *Information Technology and Societal Development* (pp. 154-182).

www.irma-international.org/chapter/theory-critical-total-history-civilization/23592

A Robust and Blind 3D Mesh Watermarking Approach Based on Particle Swarm Optimization

Mourad R. Mouhamed, Mona Mohamed Soliman, Ashraf Darwish and Aboul Ella Hassanien (2020).

International Journal of Sociotechnology and Knowledge Development (pp. 24-48).

www.irma-international.org/article/a-robust-and-blind-3d-mesh-watermarking-approach-based-on-particle-swarm-optimization/242935

US Presidential Elections on Social Media: Uses and Dependency Model

Nesma Emam Soliman and Alshimaa Mohamed Osama (2022). *International Journal of Sociotechnology and Knowledge Development* (pp. 1-15).

www.irma-international.org/article/us-presidential-elections-on-social-media/297977

Designing for Disaster: Social Software Use in Times of Crisis

Liza Potts (2009). *International Journal of Sociotechnology and Knowledge Development* (pp. 33-46).

www.irma-international.org/article/designing-disaster-social-software-use/4094

Affective Factors for Successful Knowledge Management

Peter A.C. Smith (2010). *International Journal of Sociotechnology and Knowledge Development* (pp. 1-11).

www.irma-international.org/article/affective-factors-successful-knowledge-management/39092