Pre-Service Teachers' Perceptions of Information Assurance and Cyber Security

Joachim Agamba, Idaho State University, USA

Jared Keengwe, University of North Dakota, USA

ABSTRACT

This study was designed to compare pre-service teachers' attitudes to those of general computer end-users on taking proactive measures to prevent cyber crime. Nineteen pre-service teachers, enrolled in a three-credit technology course in 2009, completed a survey instrument created by the researchers to analyze perceptions of Information Assurance (IA) and cyber security. The findings indicated a lack of best practices in IA that was no different from that of general computer end-users to protect personal electronic information.

Keywords: *Cyber Crime, Cyber Security, Information Assurance (IA), Information Security, Internet Technology*

INTRODUCTION

Cyber crime generally refers to the use of computers and the Internet to perpetrate offenses. Such crimes may be directed at individuals, institutions, communities, or society at large. Hacking, the entry point of cyber crime, is the unauthorized use of computer and network resources to access and obtain information, including writing programs to undermine computer systems' security (Hafter & Markoff, 1995).

Three schools of thought emerge on the issue of preventing cyber crime based on relevant literature. One position is that security breaches in Internet use are due to user ignorance that can be mediated by education in security training awareness (Hight, 2005). As such, "the end user is the first line of defense" (Schou & Trimmer, 2004, p. 1). Another position is that computer end-users are not experts. Therefore, software developers can prevent cyber crime by providing software that is more secure (Chandler, 2004; Marsan, 2004).

The third position seeks a middle ground: in that software developers have a responsibility to provide software products that are more effective; however, consumers are also responsible for taking proactive measures that can prevent cyber crime (Marsan, 2004). Egelman, King, Miller, Ragouzis, and Shehan (2007) argue that general computer users are usually not concerned about preventing cyber crime until they become victims. Thus, efforts towards designing and conducting studies on

DOI: 10.4018/jicte.2012040108

computer users and cyber security remains a difficult task.

Electronic security and privacy are socio-cultural phenomena from a situated perspective (Dourish & Anderson, 2006). They establish how difficult it is to narrow human issues in Information Technology (IT) into narrow constrictive categories. They also point out that rapid gains on technology do not match a human understanding of their use. As such, they argue that the focus on technology security as personal issues should be addressed as collective states in order to effectively interface human computer interaction with computer designs. This study was designed to compare preservice teachers' attitudes to those of general computer end-users on taking proactive measures to prevent cyber crime

THEORETICAL FRAMEWORK

1. What is the general end-user's attitude toward cyber security?

General computer end-users are not aware of how easy it is for a hacker to gain access to their electronic information and how they can become victims of cyber crime as a result. According to Featherstone (2009), hacking, as a data-mining culture, generally undermines security systems of individuals and organizations alike by taking advantage of vulnerabilities in software, operating systems, Internet browsers, and communication accessories by altering information to make them perform differently than they were intended.

Poor security is the primary reason why hackers are able to penetrate safeguards as well as unguarded information from computers and networks. Hackers steal information by identifying easy targets, having physical access, and evading intrusion detection systems that contain sensitive electronic information (Smith, 2009). Further, even where security structures such as a virtual private network (VPN) or a two-factor authentication exists, poor security practices can compromise such preventive measures.

Lack of good confidentiality protocol is another reason why computer end-users become easy targets for cyber crime (Adams & Sasse, 1999). Adams and Sasse explain that poor password generation and protection alone can make any system vulnerable to hacking. For example, end users generally prefer human-generated passwords to system-generated ones because the former are easy to remember, and therefore convenient; although they are also easier to crack (Adams & Sasse, 1999).

Implementing awareness training programs, such as that offered by the U.S. federal government, for employees will be beneficial. But such an approach is not reliable because professionals have a better appreciation for such training which end-users do not (Fruge, 2008; Trimmer & Schou, 2004). As a consequence, end-users become victims of hacking crimes such as credit card fraud and identity theft. Based on the literature, six proactive measures emerge that computer end users need to be aware of and practice: (1) the need to have a general knowledge of what is cyber crime, (2) awareness of the negative impact of cyber crime on society, (3) changing passwords at least twice a year, (4) avoid using the same password multiple times, (5) awareness of the need to have intrusion detection software, and (6) installing intrusion detection software in personal computers.

2. What are pr-eservice teachers' attitudes toward cyber security?

Most pre-service teachers, like general computer end-users, are not aware of the consequences of poor computer security practices (Dark et al., 2006). While there are programs to prepare undergraduate and graduate students in Information Assurance (IA) and Cyber Security, a survey of the literature spanning more than a decade of such programs in higher education indicate that they are directed specifically for students in Informatics (Bishop, 1993; Azadegan, O'Leary, Wijesinha, & Zimand, 2003; Wulf, 2003; Depalma, Frank, Gladfelter, & Holden, 2004; O'Leary, 2006; Bratus, Shubina,