

Chapter 24

Building Security Awareness Culture to Serve E-Government Initiative

Ali Maqousi

Petra University, Jordan

Tatiana Balikhina

Petra University, Jordan

ABSTRACT

Recently, many countries have adopted E-Government initiatives for providing public E-Services to their citizens. These initiatives, together with the existing and emerging private initiatives which offer E-Services, lead to a dramatic increase in the number of Internet users. This will form what is now known as E-Society. All E-Government initiatives consider citizen-centered approach, where user's security and privacy is a major issue. The level of citizen's engagement in these initiatives will depend on the extent of his/her confidence in the security system used by these initiatives. This imposes the need for developing computer security packages. These packages are intended to help users protect their assets such as information, databases, programs, and computer services from any harm or damage. The level of harm or damage that could happen to assets varies from one user to another. This variation depends on: users' awareness of possible threats, their knowledge of the source of threats, and if they are applying security controls or not. This paper aims to analyze current users' level of awareness and to propose possible methods in order to increase the level of users' awareness i.e. education, continues education, and training. This chapter is organized as follows: the first section presents an introduction, where the importance of security awareness to E-Government initiatives is highlighted and also it presents a research idea, the second section introduces the experimental design for a more comprehensive research that we are looking to carry on in later stages and specifies the objective of this stage, the third section presents results and discussions where we provide our own proposal of methods to increase the level of users awareness; finally, a conclusion is presented.

DOI: 10.4018/978-1-61520-789-3.ch024

INTRODUCTION

Importance of User Security Awareness to E-Government Initiatives

One of the most significant threats to information security could come from the system's users, because they are quite familiar with the infrastructure. It is not always dissatisfied workers and corporate spies who are a threat. Often, it is the non malicious, uninformed employee (user) ["Corporate Technology", 2008]. "E-Government" refers to the use by government agencies of information technologies (such as Wide Area Networks, the Internet, and mobile computing) that have the ability to transform relations with citizens, businesses, and other arms of government ["worldbank", 2009]. Ntiro in [Ntiro, 2000] states that E-Government has three main domains to cover: the improving government processes (E-Administration), connecting citizens (E-Citizens and E-Services), and building external interactions (E-Society). In E-Administration domain E-Government initiatives deal particularly with improving the internal workings of the public sector. However, second and third domains the Initiatives deal particularly with the relationship between government and public agencies from one side, and citizens and other institutions on the other side.

To deal with citizens as customers who consume public services means: talking to them to provide details about public service activities, listing to them to increase their input into public sector decisions and actions, and improving the services delivered to them in terms of quality, convenience, and cost. As the end user for the E-Government is a citizen, and to spread the use of public E-Services, the E-Government policy should consider a citizen-centered approach. However many people don't use E-Government for several reasons, such as unfamiliarity with ICT, lack of access, lack of training, and concerns about

privacy and security of information. As far as the privacy and security of information is of a concern in this research, there is a need for providing a way of assuring citizens that their personal information will not be compromised. This challenge could be achieved by building a user security awareness culture. In this chapter we present our proposal to build user security awareness. The proposed security policies aim to increase and maintain a certain level of user security awareness and could be implemented along side with E-Government services or/and within specific organizational administration tools.

The Internet is the most powerful means for delivering E-Government [Patricia, 2003]. The Internet represents different things to different people, it provides a powerful new framework for connection, commerce, and communication, forming what is called E-Society. However, it also brings the outside world directly into our homes or working environments. This transformation puts new requirements on our online security and safety. Being aware of these your new surroundings and thereby realizing the potential threats you may be facing is the first step in your security plan [FrontLine, 2008]. Different situations in which people could face e-threats could be classified as: home, business and academic environments.

Home users include several categories of people beginning from children and they have very diverse level of computer knowledge and security awareness. As these users face security threats at homes alone the psychology issues play here main role.

Psychologically, when we leave the safety of our homes and venture into the outside world, we instinctively raise our guard and become more alert to possible dangers. Once we back home, we lower our guard and relax. Those actions are so embedded that we do them without thinking—but staying safe and secure online requires us to keep our guard or awareness up even when inside our homes or other places where we usually feel safe["Microsoft", 2008].

6 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/building-security-awareness-culture-serve/46272

Related Content

Inclusivity and the Education of Children of Defence Forces Personnel: Exploring the Impact of Mobility and Interrupted Schooling

Ros Baumann and Henriette van Rensburg (2021). *Research Anthology on Military and Defense Applications, Utilization, Education, and Ethics* (pp. 106-124).

www.irma-international.org/chapter/inclusivity-and-the-education-of-children-of-defence-forces-personnel/284312

Uncovering the Enablers, Benefits, Opportunities and Risks for Digital Open Government (DOG): Enablers, Benefits, Opportunities and Risks for DOG

Muhammad Naeem (2019). *International Journal of Public Administration in the Digital Age* (pp. 41-58).

www.irma-international.org/article/uncovering-the-enablers-benefits-opportunities-and-risks-for-digital-open-government-dog/233926

The Place of Elderly Education Within Adult Education and Model Suggestions Regarding Elderly Education

Pelin Pekmezci and Hülya Öztop (2021). *Handbook of Research on Policies, Protocols, and Practices for Social Work in the Digital World* (pp. 508-522).

www.irma-international.org/chapter/the-place-of-elderly-education-within-adult-education-and-model-suggestions-regarding-elderly-education/279561

Contribution of Men in Safe Motherhood: A Case of Dodoma Municipality

Vincent Sebastian Pande (2020). *International Journal of Public and Private Perspectives on Healthcare, Culture, and the Environment* (pp. 27-40).

www.irma-international.org/article/contribution-of-men-in-safe-motherhood/243476

Towards an Integrated Research Framework in Public Policy-Focused Investigations

Alireza Aslani (2015). *Public Affairs and Administration: Concepts, Methodologies, Tools, and Applications* (pp. 525-537).

www.irma-international.org/chapter/towards-an-integrated-research-framework-in-public-policy-focused-investigations/127866