Information Security and Its Aapplications on the Portal of the Deanship of Library Affairs at Northern Border University

Dr. Yaser Mohammad Mohammad Al Eawy
Associate Professor of Library and Information Science – Applied College – General Curriculum Dept.- Northern Border University - Saudi Arabia.
yaseralsawy@yahoo.com – yaseralsawy@gmail.com
ORCID ID: https://orcid.org/0000-0002-3150-9497

Summary
The study aimed to assess the state of electronic security for the website of the Deanship of Library Affairs at Northern Border University, as one of the university's electronic portals, which provides distinguished knowledge services to faculty members, through the Saudi Digital Library, and the integrated automated system for libraries (Symphony) with the definition of cyber security of the university, and the most important threats The study sought to analyze the opinions of a wide sample of faculty members, towards evaluating the state of electronic security for the Deanship of Library Affairs portal, through the use of both the analytical method, as well as the survey, using the questionnaire tool, and the study sample consisted of 95 A faculty member of all academic categories and degrees, and university faculties, and the study concluded that it is necessary to work to overcome the relative slowness of the university's Internet, with the faculty members notifying the information security services through e-mail and SMS service, with the continuous updating of operating systems, Apply and use the latest anti-spyware, hacking, and anti-virus software at the university, while conducting extensive research studies towards information security services, and contracting It aims to introduce information security risks, and ways to combat and overcome them, and spread the culture of information security among faculty members.

Key words: *electronic security; cyber security; security threats; Deanship of Library Affairs; Northern Border University.*

1. Introduction

The portal is an electronic website that is a starting point for connecting to other website [1], The name of the portal came from its function as an open window through which the beneficiary overlooks the information and other services provided by the site [2], The portal is distinguished from websites with a high degree of organization, as it provides its integrated services by providing Easily, quickly and accurately access the most important sites of interest to the beneficiary [3].

Electronic security in universities means the ability to protect computers, servers, all mobile devices, associated electronic systems, internal and external networks, and data elements from all malicious attacks that hinder work [4], It can also be defined as information technology security or electronic information security, and it is the main objective of electronic security. Protecting the information and data circulated and available at the university via the Internet from tampering, sabotage or alteration [5], or from any other danger that threatens it, such as the arrival of an unauthorized person to access it [6], and tampering with its data, viewing and acquiring it, by providing many means necessary to protect it from internal or external risks The need and demand for the use of electronic security has increased after the spread of the use of the Internet, and reliance on it in business, which required the transfer of data and information across multiple networks, and thus the attempt to access and control information illegally, which necessitated the availability of many protection measures [1,3,5].

Information security consists of several main elements: confidentiality, which means preventing the knowledge of any person who is not allowed to access the data of another person, in addition to the integrity and integrity of the data [7], which means preserving the data from modification or alteration by persons who are not allowed to access it, with the intent of, or unintentionally to data that he is not allowed to access, as well as in the event that a virus reaches the computer, and modifies its data [8], this is also a violation of integrity and the lack of full protection of the information, as well as the availability of data and means the availability of complete data when it is needed so that the information is correct, accurate, unmodified or incomplete, which makes the elements of the system work properly and coherently [8,9].

Technology is therefore an urgent necessity to give organizations and individuals the necessary protection tools as everyone benefits from cyber defense programs. and financial services companies [9,10], so securing these organizations electronically, and others, is essential to keeping society operating in a safe manner.

2. Study problem

The problem of the study is that it provides an assessment of the electronic security status of one of the electronic portals of the Northern Border University, where the Deanship of Library Affairs portal is one of the vital gates, as it includes the Saudi Digital Library, as well as the bibliographic data system for all information sources

Manuscript received December 5, 2021
Manuscript revised December 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.12.26

available at the university through the integrated automated system for libraries (Symphony), and therefore the data is very important, hence the researcher's keenness to study the extent of protection provided by the university to the portal of the Deanship of Library Affairs, as no previous studies in this field have been previously conducted.

3. Study questions

The study seeks to answer the following main question:

- What are the electronic security determinants offered by the university to protect the portal of the Deanship of Library Affairs from electronic risks?

Under the main question there are several sub-questions:
- What are the forms of security risks that the portal of the Deanship of Library Affairs at Northern Border University may be exposed to?
What are the security solutions and electronic protection methods provided by the university?
- What is the current evaluation of the electronic security of the Deanship of Library Affairs portal, according to the opinions of university faculty members?

4. Importance of the study

The importance of the study is that information security at the university increases the ability to confront all electronic attacks. The application of the information security management system leads to an increase in the ability to confront any electronic attacks, in addition to the ability to provide a central electronic protection structure, where information security provides a framework for maintaining On the information security of the university, it also works to secure private information in one place, and information security helps protect all digital information and intellectual property, and thus covers the standard approach of the university, including employees, processes and technology, and this enables the university to understand risks, and adhere to controls. Security as part of daily business practices.

5. Study Objectives.

The study aims to achieve the following aspects:

1- Determining the information security policy, controls and procedures associated with it on the portal of the Deanship of Library Affairs.
2- Introducing the information security structure for the main and supporting technical environment at the university.
3- Controlling and protecting security vulnerabilities, assessing the level of vulnerability in the main servers and addressing them.
4- Participate in defining performance indicators for all activities, reviewing and developing them on an ongoing basis.
5- Identifying the extent of the university faculty members' satisfaction with information security on the electronic portal of the Deanship of Library Affairs at the Northern Border University.

6. Methodology

The study applied both the descriptive and analytical approach in relation to the definitions of cyber security, and the security risks that could face the university represented in the portal of the Deanship of Library Affairs. And about the extent of their exposure to security breaches or security attacks while using the Deanship of Library Affairs portal, where the study used the main tool (the questionnaire) to measure these trends and opinions.

7. The study theoretical framework

7.1 Cyber security

The main purpose of cybersecurity is the organization's ability to provide security solutions to protect all systems and software as well as the intranet, the external network, the Internet, and protect the organization from destructive digital attacks [1,2,11], as these organized or random attacks aim to access important and vital information, for the purpose of work cybersecurity operations in the organization include the use of a specific and integrated approach consisting of several procedures and successive stages of forms of multiple layers of protection distributed in computers or networks of all kinds, or programs or data from In order to maintain its integrity and flow in order to create an effective line of defense against various types of cyber attacks,[12] It includes the first stages of protection against electronic attacks through the creation and selection of unusual passwords so that they are strong for users, consisting of letters, symbols and numbers, provided that they are constantly changed during periodic periods with the knowledge of the user and are not stored inside the computer, and this includes not opening any untrusted attachments With files received by e-mail, and striving to create permanent backup copies of data and keep them in safe places [13]

7.2 Cyper threats

Cyber security threats come in various forms [7,8,11,13,14]:

1- A group of cyber abuses that result from individual parties or through organized groups targeting operating systems, software or data in order to gain access to information acquisition and management, and to achieve financial profit or chaos within the organization's work system.
2- That there is an organized or random electronic attack, the main objective of which is to seize and acquire information for the purpose of control.
3- Weakening the electronic systems operating in the institutions to create a state of panic and turmoil in order to create a state of inability to protect.

7.3 Malware

Malicious electronic software is a form of software designed to cause informational and physical damage [14,15], which is the most common and widespread type of electronic threats, as a criminal programmer designs and publishes it in direct or indirect ways, through direct access, or infiltration in order to destroy or disable hardware and software and enterprise operating systems, and this malware may be spread via random user downloads unintentionally or by sending them as email attachments.

There are many different types of malware, including [4,8,16,17]:
-Virus: It is a program that is designed to harm computer hardware, as it copies itself, attaches it to a normal file within the operating system, and through repeated copying spreads through the entire computer system, and the rest of the network devices, and works to destroy, erase, seize or destroy files. Partially or permanently disable their use.

-Trojan horses: a type of malicious software designed by programmers and hackers, and it is considered as malicious software that takes a form similar to trusted programs. data or capture and control it.

-Spyware: A computer program that secretly records all the procedures and stages that the user performs to manage files in order to acquire and control data.

-Ransomware: is a malicious computer program designed to take full possession of user files and data, and threaten to erase them for the purpose of requesting money or acquiring data.

-Ad-supported: is a block of adware that is used in order to spread operating system software, software and files.

-Botnets: A group of computers that have been infected with malware and spread across an organization's network, through which hackers are infiltrated to manage operations instead of the user.

-SQL injection: is a malicious type of cyber attack that is used specifically for data capture and acquisition by vulnerable software access points, data blocks and files.
- Phishing: A cyber attack by sending semi-legal emails from certified companies containing malware in order to steal data.

7.4 Protection from cyber attacks

User protection is one of the main determinants of cyber security for the organization, so that the user does not bear harm from the impact of the cyber threat, and therefore the organization seeks to upgrade cyber security measures in an integrated manner in order to protect users, systems, software [9,11], and devices through a set of encrypted protocols for all network sectors, and security is keen cyber security checks periodically for any malware, isolates and removes it from the network, and electronic security protocols focus on real-time detection of malware, through a set of experimental and behavioral analysis protocols to monitor programs, and how they perform, and security programs can also obtain developments of defensive programs through specialized research in the field of cybersecurity capable of identifying and detecting new threats and ways to eliminate them [18].

In order to get the most out of user security software, it is essential that employees learn how to use it, keep it running and update it regularly to ensure that it improves its ability to protect users from the latest cyber threats [19].

For this, organizations can protect their digital contents through the following measures: [7,14,16, 19]

-Continuous updating of applications and operating systems in order to obtain security updates.
-Use the latest antivirus software.
-Always make sure to use strong passwords, and update them periodically.
-Do not open any received attachments with emails from unknown senders.
- Avoid using anonymous and insecure WIFI networks to not be exposed to middleman attacks.

8. Study sample analysis

The questionnaire was evaluated before it was distributed by specialists in library and information sciences, and the researcher made the required adjustments by the referees. The questionnaire was also tested on 25 faculty and administrative members of the university from the two categories, and the questionnaire was distributed on a random stratified sample of university faculty members that included 95 faculty members.

8.1 Analysis of the results

The questionnaire was evaluated before it was distributed by specialists in library and information sciences, and the researcher made the required adjustments by the referees. The questionnaire was also tested on 25 faculty and administrative members of the university from the two categories, and the questionnaire was distributed on a random stratified sample of university faculty members that included 95 faculty members.

8.1 Analysis of the resul

The data and its outputs were reviewed by the researcher, with the statistical data checked after analyzing it through the statistical program SPSS.

Table (1) Distribution of the research sample members according to gender

Type	Frequencies	Percent
Male	51	53.7%
Female	44	46.3%

Table (2) Distribution of the research sample members according to the academic degree

Academic Degree	Frequencies	Percent
Professor	9	9.5%
Associate Professor	18	18.9%
Assistant Professor	47	49.4%
Lecturer	21	22.1%
Total	95	%100

Table (3) Distribution of research sample members according to colleges

College	Frequencies	Percent
Science	32	33.7%
Education and Science	13	13.7%
Business Administration	22	23.1%
Medicine	16	16.8%
Engineering	12	12.6%
Total	95	100%

#	Standard	Average	Deviation	Level
1	Easy access to the Deanship of Library Affairs portal	82.1%	2.87562	Good
2	Availability of all services and access points	79%	2.23021	Medium
3	Slow to use the portal	23%	2.87921	Poor
4	Availability of the Internet through the university campus	91.5%	2.78632	Excelent
5	Vulnerability of the service to electronic hacking or cyber-attack	7.3%	0.01789	Very Poor
6	Receiving suspicious emails via university mail	3.1%	0.01235	Very Poor
7	The extent of confidence in the information security of the university	87.4%	2.78621	Very Good
8	Evaluation of the information security performance of the Deanship of Library Affairs portal	81%	2.36195	Good

9. Discussion

The results of the statistical analysis of the study show a high rate of acceptance and the availability of security protection service, with a low rate of exposure to security attacks or exposure to suspicious e-mail to the Deanship of Library Affairs portal, according to the following main elements:

Regarding the feature of accessing the portal of the Deanship of Library Affairs on the main university website, the results indicate a high rate of responses from faculty members, as 78 faculty members answered with ease of quick and safe access to the portal of the Deanship of Library Affairs, representing approximately 82.1% of the study sample, As for the availability of services and access points, the responses of the faculty members indicate a

medium degree of acceptance, where 75 of the study sample answered yes, and they represent approximately 79% of the study sample, While 22 faculty members answered that there is a slowdown in using the portal site, at a rate of 23%, and this indicates a high percentage of satisfaction with regard to the speed of using the portal site, as it is considered that those who answered yes are 73 faculty members, representing approximately 77% of the study sample, With regard to the availability of Internet service on the university campus, the results indicate a very large increase for those who answered yes, as 87 faculty members responded with the availability of the service, representing approximately 91.5%, which is a high percentage indicating the university's keenness to provide the service on a continuous and effective basis, While the results indicate the low exposure of the website of the Deanship of Library Affairs to exposure to electronic attacks, hacking or espionage, from the point of view of the faculty members, 7 faculty members indicated their exposure to this, representing approximately 7.3% of the study sample, and this indicates the strength of the procedures of protection services Electronic security at the university, With regard to receiving suspicious emails via university e-mail, the responses of faculty members indicate that 3 faculty members, representing approximately 3.1% of the study sample, received suspicious emails, but they do not have to carry a security threat related to exposure. informational cyber attacks, The results also indicate a high degree of confidence in information security at the university, where 83 faculty members, representing 87.4% of the study sample, indicated yes, which is a trustworthy percentage and indicates a high level of information security services at the university, In general, with regard to the extent of the faculty members' satisfaction with information security services at the website of the Deanship of Library Affairs at the Northern Border University, there is a high percentage of the level of satisfaction, where 77 faculty members from the study sample answered yes, representing approximately 81%, which is a high percentage indicating that The quality of the information security services provided by the university.

10. Results

Based on the analysis of the opinions of faculty members towards information security services for the portal of the Deanship of Library Affairs at the university, the following results can be reached:

1- The university's keenness to provide information security services for electronic portals.
2- An update of the electronic protection programs for the university's website and all available software and data.
3- Update operating systems and include information security protections on a regular basis.
4- Easy access to the Deanship of Library Affairs portal, and it provides all safe elements for operation.
5- The availability of high and continuous Internet service in all university campuses.
6- Availability of sufficient internet speed for university faculty members.
7- The low exposure of the portal of the Deanship of Library Affairs to electronic attacks.
8- Low exposure of faculty members to receiving suspicious emails.
9- The high level of confidence in the university's information security services.
10- The high degree of satisfaction of university faculty members towards information security services.

11. Recommendations

By analyzing the results of the study, the following recommendations can be suggested:

1.Working to overcome the relative slowness of the university's Internet to provide faster service to all faculty members.
2.The necessity of notifying faculty members through e-mail and SMS about all that is new about information security risks, and ways to overcome them.
3.The need to constantly update operating systems.
4.The necessity of applying and using the latest anti-spyware, piracy, and virus programs at the university.
5.Conducting extensive research studies towards information security services at the university on an ongoing basis.
6.Holding a workshop through the university administration for faculty members to introduce information security risks, and ways to combat and overcome them.
7.Spreading a culture of information security among faculty members, and raising awareness about the safe use of e-mail, and secure access to websites.

Acknowledgment

The authors gratefully acknowledge the approval and the support of this research study by grant no. 7626 from the Deanship of Scientific Research at Northern Border University, Arar, K.S.A.

References

[1] Green, N., Liu, M., Murphy, D. (2020). Using an Electronic Resume Analyzer Portal (eRAP) to Improve College Graduates Employability. Information Systems Education Journal, 18(3),28-37.

[2] Kelly, B., McCormack, M., Reeves, J.; Brooks, D., O'Brien, J. (2021). 2021 EDUCAUSE Horizon Report: Information Security Edition. EDUCAUSE. ISBN: 978-1-933046-07-5

[3] Spitzer, S. (2012). Make That to Go: Re-Engineering a Web Portal for Mobile Access. Computers in Libraries, 32(5),10-14.

[4] Saghapour, M., Iranmanesh, M., Zailani, S., Goh, G. (2018). An Empirical Investigation of Campus Portal Usage. Education and Information Technologies,23(2),777-795.

[5] Hufe, Mark J. (2014). Building Information Security Awareness at Wilmington University. ProQuest LLC, Ed.D. Dissertation, Wilmington University, Delaware. ISBN: 978-1-3039-1278-8

[6] Karagozlu, D. (2020). Determination of Cyber Security Ensuring Behaviours of Pre-Service Teachers. Cypriot Journal of Educational Sciences,15(6),1698-1706.

[7] Finkel, E. (2019). Creating a Cyber-Secure Campus. Community College Journal, 89(4), 11-15.

[8] McDermott, M., Reeves, J., Mendez, G., Capo, B., Karp, J. (2019). Maintaining Privacy and Security in Cyberspace: What Everyone Needs to Know. Distance Learning,16(3),16-26.

[9] Taylor, N. (2015). Information at the Nexus: Young People's Perceptions of Government and Government Websites. ProQuest LLC, Ph.D. Dissertation, University of Maryland, College Park. ISBN: 978-1-3394-7562-2.

[10] Carlon, S. Carter, M. Stephenson, J. (2017). Pilot Study of a Parent Guided Website Access Package for Early Intervention Decision-Making for Autism Spectrum Disorder. Australasian Journal of Special Education,41(2),141-156.

[11] Johnson, C. (2019). University of South Wales National Cyber Security Academy -- Creating Cyber Graduates Who Can 'Hit the Ground Running': An Innovative Project Based Approach. Higher Education Pedagogies, 4(1), 300-303.

[12] Rajab, M. (2019). The Relevance of Social and Behavioral Models in Determining Intention to Comply with Information Security Policy in Higher Education Environments. ProQuest LLC, Ph.D. Dissertation, Eastern Michigan University. ISBN: 978-1-3921-5302-4.

[13] Frontera, P.; Rodriguez-Seda, E. (2021). Network Attacks on Cyber-Physical Systems Project-Based Learning Activity. IEEE Transactions on Education, 64(2),110-116.

[14] Gross, M., Ho, S. (2021). Collective Learning for Developing Cyber Defense Consciousness: An Activity System Analysis. Journal of Information Systems Education, 32(1),65-76.

[15] Alqarni, Amani. (2017). Exploring Factors That Affect Adoption of Computer Security Practices among College Students. ProQuest LLC, Ph.D. Dissertation, Eastern Michigan University.

[16] Davis, M. (2017). Ingress in Geography: Portals to Academic Success? Journal of Geography,116(2), 89-97.

[17] Bringula, R., Basa, R. (2011). Factors Affecting Faculty Web Portal Usability. Educational Technology & Society,14(4), 253-265.

[18] Monk, N. (2015). Portal Pedagogy: From Interdisciplinarity and Internationalization to Transdisciplinarity and Transnationalization. London Review of Education,13(3), 62-78.

[19] Manca, S. (2018). ResearchGate and Academia.edu as Networked Socio-Technical Systems for Scholarly Communication: A Literature Review. Research in Learning Technology, 26.

Yaser Mohammad Al Sawy- Associate professor of Library and Information Science, Applied College – General Curriculum Dept.- Northern Border University - Saudi Arabia, Advisor for the vice presidency, Advisor for the Deanship of Scientific Research, Advisor for Kuwait Institute for Scientific Research (KISR) (Kuwait), Director of Acquisition Unit at Arab Open University (Kuwait), Information Specialist at Awqaf Public Foundation (Kuwait).