مجلة العلوم البحتة والتطبيقية
Journal of Pure & Applied Sciences
www.Suj.sebhau.edu.ly ISSN 2521-9200
Received 12/01/2018 Revised 08/02/2018 Published online 30/06/2018

Insider Attacks against Non-Financial Organizations

Othoman Elaswad , *Mahmoud Aljdawi
Department of Computer science, Faculty of Information Technology, University of Sebha, Libya
*Corresponding author: mah.aljdawi@sebhau.edu.ly

Abstract Recently, several public and private sectors such as governments, companies and universities use Information and Communication Technologies (ICT) to transform paper-based systems into electronic services. E-service systems may expose to various electronic attacks such as identity theft and phishing attacks. Attacks are classified into insider and out sider attacks. Several studies show that, insider attackers are more dangerous than out sider attackers. Non-financial organizations such as civil registers and universities organizations have sensitive and valuable information may expose to insider attacks. In this paper, we select Student Information System at Sebha University-Faculty of Science as a case study in order to investigate the susceptibility of end users to insider attacks using social engineering and phishing techniques. We performed two steps to achieve our goal. Firstly, we develop a conceptual model of an attacker instead of performing a real attack. Secondly, we made a survey questionnaire in order to assess to which extent end users are susceptible to insider attack based on the conceptual model.
The analysis of end user's responses using statistical tests show that, large number of end users at the target organization is susceptible to insider attack easily. Weak of computer skills and lack of information security culture are the most factors enable insider attack to success attacking the organization. Therefore, Sebha University-Faculty of Science needs to improve the skills as well as security culture of their end users to protect end user's records as well as resources. Training end users to create their emails and their online accounts by themselves is one possible way to improve skills. Awareness end users with risks of electronic crimes by seminars are another way to improve security culture.
Keywords: Cyber security, Phishing Attacks, information security threatens.

الهجمات الداخلية ضد المنظمات غير المالية

عثمان أبوبكر الأسود و *محمود صالح الجداوي
قسم علوم الحاسب– كلية تقنية المعلومات– جامعة سبها، ليبيا
*للمراسلة: mah.aljdawi@sebhau.edu.ly

الملخص في الآونة الأخيرة ، العديد من القطاعات العامة والخاصة مثل الحكومات والشركات والجامعات استخدمت تكنولوجيا المعلومات والاتصالات لتحويل أنظمتها الورقية التقليدية إلى خدمات إلكترونية. قد تتعرض هذه الأنظمة لعدة هجمات إلكترونية مختلفة مثل سرقة الهوية وتصيد المستخدمين. تصنف الهجمات إلى هجمات داخلية وهجمات خارجية. تشير العديد من الدراسات إلى أن المهاجمين الداخليين أكثر خطورة من المهاجمين الخارجيين. المنظمات غير المالية مثل مصلحة الأحوال المدنية والجامعات لديها معلومات حساسة وقيمة قد تعرضها لهجمات من الداخل. في هذه الورقة ، قمنا باختيار نظام معلومات الطالب بكلية العلوم – جامعة سبها كنموذج لدراسته وذلك من أجل التحقق من احتمال تعرض مستخدمي هذا النظام لهجمات داخلية باستخدام تقنيات الهندسة الاجتماعية والتصيد. قمنا بعمل خطوتين لتحقيق هدفنا. أولاً : قمنا بتطوير نموذج مفاهيمي للمهاجمين بدلاً من القيام بهجوم حقيقي. ثانياً ، قدمنا استبياناً إستقصائياً لمستخدمي النظام من أجل تقييم إمكانية تعرضهم لهجوم داخلي بناءً على النموذج المفاهيمي. تم تحليل إجابات مستخدمي النظام على أسئلة الإستبيان بواسطة اختبارات إحصائية ، نتج عن هذا التحليل أن عدداً كبيراً من المستخدمين هم عرضة للهجوم من الداخل بسهولة. يعد ضعف المهارات الحاسوبية والافتقار إلى ثقافة أمن المعلومات من أهم العوامل التي تمكن من نجاح الهجمات الداخلية. لذلك ، تحتاج كلية العلوم بجامعة سبها إلى تحسين مهارات مستخدمي نظام معلومات الطالب والرفع من ثقافتهم الأمنية لحماية سجلات المستخدمين وموارد الكلية. يعد تدريب مستخدمي النظام على إنشاء رسائل البريد الإلكتروني الخاصة بهم وإدارة حساباتهم عبر الإنترنت بأنفسهم إحدى الطرق الممكنة لتحسين مهاراتهم. إعطاء مستخدمي النظام محاضرات وندوات للتوعية بمخاطر الجرائم الإلكترونية يعتبر طريقة أخرى لتحسين ثقافة أمن المعلومات لدى هؤلاء المستخدمين.

الكلمات المفتاحية: أمن الحواسيب ، هجمات التصيد ، تهديدات أمن المعلومات.

Introduction

During last two decades several private companies, universities and governments use Information and Communication Technologies (ICT) to transform paper-based systems into electronic services such as e-commerce, e-government and online banking. E-services are defined as "services that are produced, provided, and/or consumed through the use of ICT networks such as Internet-based systems and websites"[1]. Therefore, to automate manual routines, information systems are

important tools in public and private sectors. The most common features of such transformation are improve service delivery, increase transparency and cost-effective[2]. On the other hand, online accounts and e-service systems are exposed to various attacks as a result the number of cyber-crimes has been increased.

Attacks are classified into outsider and insider attacks depend on whether an attacker belongs to the attacked system or not. Several researches investigate external attacks against financial organizations. For example, Havasi shows that security vulnerability, lack of knowledge of end users and user interface are the major issues challenge electronic banking and may leads to the failure of bank transitions [3]. On the other hand, non-financial organizations also, have valuable information needs to be protected against attacks specially, insider attacks.

Insider attacks are considered the most difficult problem to deal with, because an insider attacker has much information about the target organization than outsider attackers. The most common techniques use to attack online application are Cross-Sit Scripting, SQL injection, Denial-Of-Service and Web spoofing[4][5][6].For instance, in 2008, one study reported that the number of phishing organizing electronic crimes cases increased by 300% every year [7]. Each attack site may be used to defraud hundreds or thousands of victims, and it is likely that many attack sites are never detected. The main mechanisms of Web spoofing include phishing and social engineering attacks. Kevin Mitnick defines Social Engineering (SE) attack as "using influence and persuasion to deceive people and take advantage of their misplaced trust in order to obtain insider information"[8].Researchers have proved that, human end users are the weakest link in the security chain. That means secure systems may be broken by their own users. Therefore, it is easier for an attacker to gain unauthorized access to the information and communications technology infrastructure of an organization through an individual, rather than trying to penetrate a security system.

This paper aims to investigate insider attacks against non-financial organization. To achieve our goal we develop a Faculty Insider Attack (FIA) Model to analyze the case study. We select Student Information System (SIS) at Sebha University-Faculty of Science as the case study. As the weakest link of security chain is an end user, we would examines the extent to which end users are susceptible to insider attacks using social engineering and phishing techniques to attack the specified organization information system.

Related work

Several researchers investigate electronic crimes against financial organizations. For instance, in 2005, Lynch reported that, financial records of more than 100,000 customers at Bank of America Corp. had been stolen by their bank employees and sold to collection agencies[9]. This reflects that many researches focus on cyber security against financial organization while non-financial organization may exposed as well to the attacks. So, it is important to investigate security threatens against non-financial organization. Further, it is clear from the above example that, the attack was performed by insider attackers. Researchers show that, security approaches applicable to the "outsider" may not be equally effective for insiders[10].

Probst defines insider attacker as "an individual with privileges who misuses them or whose access results in misuse". Access to the system, Knowledge and trust are the most common properties of insider attackers[10].

The most common and effective means to perform insider attacks against information systems is Social Engineering method and phishing attacks. Because attackers have realized that it is easier to gain unauthorized access to the information and communications technology infrastructure of an organization through an individual, rather than trying to penetrate a security system[8][11].

This paper aims to investigate insider attacks against non-financial organization. To achieve our goal we develop a Faculty Insider Attack Model to analyze the case study. We select Student Information System (SIS) at Sebha University-Faculty of Science as the case study. As the weakest link of security chain is an end user, we would examines the extent to which end users are susceptible to insider attacks using social engineering and phishing techniques to attack the specified organization information system.

Conceptual Model of Faculty Insider Attack (FIA)

Concepts and Background of Insider Attack

Insider is defined as all persons that have access to an organizations information system including people such as employees. Therfore, Insider attack is defined as any authorized user who performs unauthorized actions that result in loss of control of computational assets[10][12].

The chance of insider attackers to attack an organization successfully is much more than out sider attackers due to various chracteristics[10][12]. The key characteristics as follows :

- Insiders can be trusted because they are assumed to be part of the organization's culture.
- Insiders have legitimate access to the organization's information system.
- Insiders have knowledge of information and services used in an organization such as security measures and policies inside an organization. So, they may have the ability to violate them.

FIA Model

To avoid performing a real attack against an organization, we develop a faculty insider model attack. FIA model aims to clarify attack motivation, actions, techniques and risks in order to understand the factors impact the success of such attack. As shown in the model the attack starts by exposit vulnerability of end users using various techniques. Both techniques focus on end user's behaviors. Impersonating either student or lecturer as shown in the model will enable an attacker performing unauthorized access. The consequence

of unauthorized access leads the organization to various risks. The following subsections will clarify attacks process and techniques.

FIA Attack Motivation

As a lecturer has more access privileges than a student so, in this model we assume an insider attacker is a student because, often an attacker try to gain more access privilege than it has or at least similar privileges level to gain benefited. Therefore, the motivation of FIA attack depends on impersonating student or lecturer.

There are various cases where FAI attack impersonate student. One possible scenario is that, if the policy of the university restricted the number of student in each course then an attacker attacks registered students for that course in order to update the impersonator's record by deleting the course and later adding the course to attacker's record using real credential of the attacker. Such threatens affects the accuracy of data as a result the integrity of student's record is affected. Another possible scenario motivate the attacker is to disclose private information of other students such as results and previous courses marks.

The most danger risks exist when an attacker impersonate lecturer as a lecturer has more access privileges than an attacker. This motivates an attacker to impersonate a lecturer and gain much authority such as updating marks of students. Further, an attacker may disclose and illegally update lecturer's record in order to place a lecturer in trouble with the organization.

FIA techniques

It is clear from the FIA model that an attacker focus on exploit end user characteristics behaviour. Therefore, Social Engineering and Phishing techniques are the most suitable for such attack. As the social relationship trust among students is much stronger than student-lecturer trust relationship, so Social engenering technique is used by FIA attack to impersonate other students. In general, computer skills level

Figure 1 shows FIA model

various between end users so, students with lack computer skills may ask one of their close friends to creat either an email or an account on the orgnization web application under his/her behalf. In such cases an attacker use trust relation to exploit such weakness. Another possible scenario is that, some end users do not change default password so, attackers may use trust relatioship to aknowledge by such information.Students may writedown thierpassword on a piece of paper or store it on their mobile device or laptop if the password is difficult to remember. Those students are exposed to social engineering attack because, trusted friends may share use of their own devices.Lack of internet connection also may exploit by the attacker because, some studentsmay asking their trusted friends to act on their behalf so, they give their credentials(user name, password). Therefore, such threatness increase the possability of success lunching FIA using social engineering technique.

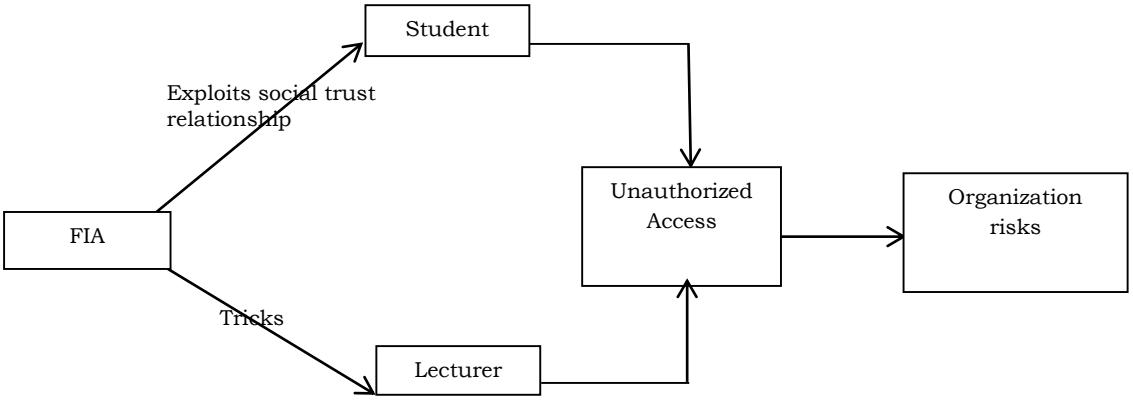

Figure. 1 shows FIA model

The second type of the FIA attack is based on the deception as shown in the model. As we assume the attacker is a student and the social relationship between students and lecturers is limited so the best technique for such attack is phishing attack. To perform phishing attack an attacker requires the following steps

- Specify the target to be attacked
- Collect information related to the specified target
- Design a strategy that enable to convince the specified target
- Send a phishing email to the specified target
- Lunch the attack when getting the credential (user name and password)

The first requirement depends on the motivation of the attacker which explained at the beginning section. The second requirement concerns about the information. Information is classified into three groups include public information, private information and secret information. It is easy for insider attack to get public information such as the name of the target user and the department. Private information can be defined as information known by a group of people such as family, organization, friends so it is not known by all people. National Identity number (NID), mobile phone number, passport number and bank account number are examples of private information. Collecting private information is more difficult than getting public information, but it is

possible. For instance, with few attempts within NID website, it is possible to retrieve the required NID number[13].Social Networks such as Facebook is another source of personal information such as mobile number. The third type of information is the secret information such as the password of an email account. This type of information is the most difficult to get. Therefore, in our case study we can build a record of personal information contains name, department, NID number, auditing number, number of children, mobile phone number and name of courses thought by the target lecturer. NID number, auditing number and number of children are collected from NID website while mobile number is collected from the department or Facebook. This information are sufficient to convince the specified target that the email is sent by the organization to verify the correctness of the information and no need to reply if all of them are valid. One possible trick is that, place wrong random bank account number to enforce the target user click the link to update the invalid information. As the target user clicks the link in the email, a web page under the attacker control is displayed. The attacker web page should be similar to the login page of the organization system to make it as a legitimate login page. This could be done by use the logo image of the organization and close similar URL. Finally, if the target user enters the credential then an attacker can impersonate the target user otherwise, an attacker try to repeat the process until convince the target user. Therefore, performing phishing attack depends on the ability of an attacker to convince the target user by make the email appear as legitimate email.

Impact of end users on the organization

Attackers may exploit vulnerability by end users to attack organization valuable information. As we explore in the motivation section that, FIA attack may modify student's record by deleting or adding courses. Furthermore, an attacker may impersonate a lecturer and modify the marks of students belongs to that course. These modifications affect the accuracy of information and as a result affect the integrity of valuable information. Another risk may originate by FIA affects the confidentiality of information such as displaying either student's result or lecturer's private information. Therefore, the organization suffers from FIA attack and as a result the reputation of the organization is effected due to unauthorized modification is performed. The following are some impacts of the attacks on the organization and their end users.

- Abuse students as well as lecturer by displaying their sensitive information through social networks as an example.
- Financial lost. When an organization investigating lunched attack, it provides financial support for a team that investigates threatens
- Accuracy of employee's records is affected due to unauthorized access.
- End users lost trust to deal with organization system.

Due to the above impacts the organization system may be terminated.

Factors impacton success implementing insider attack

Based on the techniques use by FIA model, human characteristics is the main factor exploit by the attacker. This paper categorize human characteristics that leads to threatens into four factors as follows

- Computer skills
- Social trust relationship
- Awareness of information security culture
- Availability of access connection

Methodology

This study focuses on users who use the web application at Sebha University Faculty of Science. To evaluate the susceptibility of the end users against the techniques used by FAI attack, we performed selected SIS system as a case study. The following subsection will describe the case study and the method used to collect information.

Case study

Due to rapid advance in Information and Communication Technology (ICT), Sebha University has adopted Informatics Development Project (IDP) in order to automate manual routine to electronic services using Internet and web application.IDP project consists of a number of projects include Student Information System (SIS), Library Management System (LMS), and E-Learning Management System.

In this study we focus on The Student Information System (SIS) as the only one project has been working as pilot phase. To gain access to the system, either a

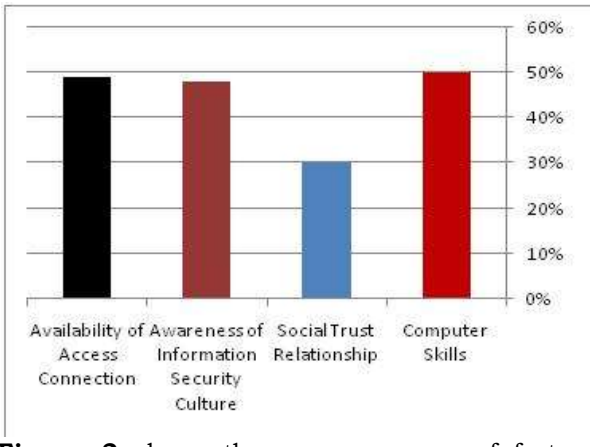

Figure. 2 shows the average means of factors impact on success lunching an attack

student or a lecture needs to register. Gmail account is considered as an initial requirement for a user to register on SIS system. Then, a user should fill other personal and academic information beside the Gmail account. The system generates user name and password. The user name is mix of the first and last name. If the user is a student, then the default password will be the word "password", while a lecture has the right to choose a password. After registration, a student can access the system to register courses or display results while a lecture permits to enter courses marks.

Survey Questionnaire

A questionnaire survey was used. The questionnaire consisted of 20 questions excluding demographic information. The demographic information questions consist of four questions include positions, gender, age and department. The questionnaire was built based on the variables impact on the success implementing FAI attack as described in the above model section. Therefore, the questionnaire questions are classified into four groups. The first five questions collecting information about end user's skills. Questions from six to twelve collect information about social trust relationship among end users. Questions from 13 to 16 collect information about information security awareness among end users while the last four questions collect information about availability of access connection variable.

We distributed an initial version of a survey questionnaire to three computer security professionals in order to verify whether the questions sufficient to assess the identified variables. Then, we refined and distributed the questionnaire among 25 of end users to examine the clarity of questions by the end users before the final distribution. These variables are measured using 5-point Likert scale, which ranged from strongly disagree to strongly agree. Then, we tested the reliability of the collected participant's responses using Kronbach's Alpha test. The ratio was 0.72 which is much higher than the minimum acceptance of reliability or stability of 0.60 .Therefore, the stability of the tool and the correlation between the answers is good and statistically acceptable.

Discussions

A total of 124 participants completed the survey over a period of 14 days. Lecturers and students from all different departments at Sebha University Faculty of Science are included. The number of lecturers participated in the survey is 24 lecturers which represent about 25% of lecturers at Sebha University Faculty of Science. The number of students participated in the survey is 100 students which represents about 15% of all students at the same organization.

Figure 2 shows the average mean of each factor that has an impact on success implementing insider attack based on the participant's responses.

It is clear from Fig. 2 that more than 49% of end users are limited with computer skills. In this context we defined computer skills as the ability of the end users to create their emails by their own and be able to interact directly with the system without asking others help. The most measures used in this paper to assess computer skills are the ability to create an email, the ability to interact directly with the system, knowledge of legitimate link to the system and knowledge to contact service provider. Based on the participant's responses we found that, 43% of end users are unable to create emails by themselves. The majority of end users who do not have the skills to create emails are students with 38% while few are lecturers with 5%. Therefore, large number of students as well as part of lecturers who are limited with skills to create emails will use their social relationship by asking others to create their emails under their behalf. As a result such groups are exposed to social engineering attacks.

Further, 32% are unable to interact with the system by their own. All of them are students. It reflects that, they give their credentials (username & password) to others who act under their behalf. Also, such groups are exposed to social engineering attack as their credentials will be given to trusted people such as friends, relatives or might be given to a third party such as a public service agency. So, if something wrong happen the system can prove that the credential has been used but cannot identify the person who impersonates the real user. Furthermore, only 16% of participants precisely identify the link to the system, 4% of participants are not sure while 80% of participants do not know the link. Such founding reflects the chance of phishing attack by exploit lack of precise knowing the link. As insider attack can get much information about target to be attacked so, both end users include lecturers and students are exposed to phishing by exploit lack of distinguishing illegitimate links from legitimate. Therefore, the scenario described in the FAI technique section is possible to lunch success attack. The situation will be more risk if the target is a lecturer as explained in the above section. We observed that 21 out of 24 of lecturers do not know the legitimate link to the system. That means large number of lecturers may expose to fishing attack.

Limited computer skills described in the above paragraphs is one among other factors enable social engineering attacks. Individuals with qualified computer skills may also, ask others help when they are busy with other business or sickness. Based on the questionnaire survey responses, 49% of participant's response agreed to ask their close friends to act under behave. It reflects that, large number of end users disclose their credentials to others while they are able to interact directly with the system. 29% of lecturers (7out of 24) ask others to act on their behalf while 54% of students (54 out of 100) do so. There are various reasons enforce end users to perform such negative habits. Time restriction for registering courses or input marks may indirectly enforce users to perform such negative habits. Lack of information security awareness among end users may enable sharing credentials. For instance, 34% of student participants and 13% of lecturers agreed to disclose their private information to their close friends such as disclose their results, disclose their NID number and student registration number. Disclosing such private information reflects the possibility of lunching success social engineering attack.

Table 1 shows participant's response to information security awareness questions

Questions	Agree	Disagree	I do not know
	Out of 124		
Created an email for close friends within the organization	36	50	38
Registering courses or input marks under behalf of others	73	18	33
Using easy passwords	68	33	23
Using one password for all my accounts	41	56	27
Verify email sender's identity	76	26	22
Configure mail filter to prevent unknown mails	60	42	22

We converted participant's responses to information security awareness into 3 scales instead of 5 scales by combining agree and strongly agree into agree column while disagree with strongly disagree are combined in another column as shown in table 1. 29% of participants ensure that they created emails for other end users within the organization. Furthermore, 59% of participants ensure that they registered courses under behalf of their friends. 33% of lecturers (8 out of 24) ask others to act on their behalf to enter marks. Such founding indicates sharing passwords among large number of end users within the organization and as a result impersonate students using social engineering attack is possible as well as lecturers. Users with limited computer skills may give their credentials to others because they are unable to interact with the system but qualified users able to interact directly with the system so, we refer sharing of passwords among qualified end users to lack of information security awareness specially that 55% of participant agreed to use easy passwords to access the system.

It is clear from table 1 that 20% of participants do not verify sender's identity of coming email and 34% do not filter coming mails. More additional, 80% of participants do not identify the legitimate link to the system as described in the above paragraphs. Therefore, large numbers of end users are exposed to phishing attack due to their limited computer security skills and awareness.

Affordability of access connections such as availability of Internet and Internet speed as well as the availability of devices is another factor that indirectly enforces end users to ask friends act under their behalf. Based on the participant's response to questions related to the affordability of access connections, we found that 20% of participants do not have Internet connection and 31% do not have either PCs or laptops. It is clear from data collected that all lecturers have Internet connection while few students do not .On the other hand, 50% of participants who has an Internet connection but the Internet speed is slow.

Based on the discussion above we could summarize the characteristics of end users within Students Information System at Sebha University-Faculty of Science as follows

- Half of end users with limited computer skills as they are unable to create email by their own.
- More than half of end users share their credentials.
- Most of end users do not know the legitimate link to the SIS system.
- Lack of information security awareness and skills as they either verify email sender or filtering coming mails.
- Large number of the end users does not have Internet connection as a result leads to lack of access connection.

Due to the above user's characteristics one might say that both end users include students and lectures are exposed to attacks described in the developed model above.

Recommendations and lessons learned

The chance of insider attackers to attack an organization successfully is much more than out sider attackers As described in the concept and background section. Furthermore, several researchers shows that, it is easier for attackers to gain unauthorized access to the information and communications technology infrastructure of an organization through an individual, rather than trying to penetrate a security system [8][11]. Therefore, the policy makers at Sebha University-Faculty of Science and other similar organizations who transform from paper-based systems into electronic systems should not consider only security software and tools to protect their systems. So, assessment end user's characteristics are equivalent important as security tools in order to protect electronic systems. Based on the founding of the paper and the identified end user's characteristic in the above section, both end users include lecturers and students at the target organizations are susceptible to social engineering and phishing attacks. But impersonate a lecturer exposed the organization to much risks because; attacker will gain more permission than it has. So, user name & password is not the suitable user authentication scheme in this case due to the identified end user characteristics and the well-known short come of password technique. Therefore, we suggest replacement of the existing user authentication mechanism especially for the lecturers with other authentication mechanisms such as one time password and finger print authentication in order to resist electronic attacks discussed above. Additionally, we recommend the following:

- Giving short practical training on Internet applications such as creating emails & browser's features.
- Organization needs to introduce the new system such as Student Information System

(SIS) at Sebha University-Faculty of Science. All end users should learn how to interact with the system, identify the legitimate link to the system, permissions of each end user group and features of the system.

- Educate endusers with information security awareness and skills by giving seminars on password management systems, risks of electronic applications and common attacks techniques.
- Ensure affordability of access connection such as develop a laboratory with PCs, laptops and Internet connection for end users to access the system.

Conclusion

Non-financial organizations such as civil registers and universities have sensitive and valuable information may expose to insider attacks. In this paper, we select Student Information System at Sebha University-Faculty of Science as a case study in order to investigate the susceptibility of end users to insider attacks using social engineering and phishing techniques. We performed two steps to achieve our goal. Firstly, we developed a conceptual model of an attacker instead of performing a real attack. Secondly, we made a survey questionnaire in order to assess to which extent end users are susceptible to insider attack based on the conceptual model.

We analyzed the questionnaire survey responses using descriptive statistical method. Based on the analysis we realized that large number of the end users is susceptible to social engineering and phishing attacks. Limited computer skills, lack of access connection and lack of information security awareness are the most common factors enable mentioned attacks.

Based on the above discussion and founding we suggest replacement of the existing user authentication scheme with other user authentication schemes such as one time password and finger print authentication especially for lecturer's group as they have more permission than students. We also recommended some steps to be done to improve the above factors in order to resist such electronic attacks.

References

[1]- A. Scupola, Cases on Managing E-services. IGI Global, 2008.

[2]- J. Holgersson and F. Karlsson, "Public e-service development: Understanding citizens' conditions for participation," Government Information Quarterly, vol. 31, no. 3, pp. 396–410, 2014.

[3]- F. Havasi, F. A. Meshkany, and R. Hashemi, "E-banking: Status, implementation, challenges, opportunities," IOSR Journal of Humanities and Social Science, vol. 12, no. 6, pp. 40–48, 2013.

[4]- J. Liu, X. Liu, B. Zheng, and J. Tang, "Design and implementation of code security inspection system based on SVN," in Computer Science and Service System (CSSS), 2011 International Conference on, 2011, pp. 330–333.

[5]- W. Maes, T. Heyman, L. Desmet, and W. Joosen, "Browser protection against cross-site request forgery," in Proceedings of the first ACM workshop on Secure execution of untrusted code, 2009, pp. 3–10.

[6]- T. Alexenko, M. Jenne, S. D. Roy, and W. Zeng, "Cross-site request forgery: attack and defense," in Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE, 2010, pp. 1–2.

[7]- O. Delgado, A. Fuster-Sabater, and J. M. Sierra, "Analysis of new threats to online banking authentication schemes," in X Spanish Meeting on Cryptology and Information Security-RECSI, 2008, pp. 337–344.

[8]- F. Mouton, L. Leenen, M. M. Malan, and H. S. Venter, "Towards an ontological model defining the social engineering domain," in IFIP International Conference on Human Choice and Computers, 2014, pp. 266–279.

[9]- D. M. Lynch, "Securing Against Insider Attacks.," Information Systems Security, vol. 15, no. 5, pp. 39–47, 2006.

[10]- J. Hunker and C. W. Probst, "Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques.," JoWUA, vol. 2, no. 1, pp. 4–27, 2011.

[11]- K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Social engineering attacks on the knowledge worker," in Proceedings of the 6th International Conference on Security of Information and Networks, 2013, pp. 28–35.

[12]- W. Cornelissen, "Investigating insider threats: problems and solutions." University of Twente, 2009.

[13]- O. Elaswad and C. D. Jensen, "Identity management for e-government Libya as a case study," in Information Security for South Africa (ISSA), 2016, 2016, pp. 106–113.