A Pilot Analysis of Factors Affecting Defense Against Social Engineering Attacks in the Armed Forces Environment

Muhammad Farhan Shahrom[1], Nurazean Maarop*[2], Ganthan Narayana Samy[3], Noor Hafizah Hassan[4], Fiza Abdul Rahim[5], Pritheega Magalingam[6], Norshaliza Kamaruddin[7]

Universiti Teknologi Malaysia
[1]farhan.shahrom@gmail.com, [2]nurazean.kl@utm.my, [3]ganthan.kl@utm.my, [4]noorhafizah.kl@utm.my, [5]fiza.abdulrahim@utm.my, [6]pritheega.kl@utm.my, [7]norshaliza.k@utm.my

Article history

Received:
14 April 2021

Received in revised form:
25 April 2021

Accepted:
15 May 2021

Published online:
26 June 2021

*Corresponding author
nurazean.kl@utm.my

Abstract

Social engineering is a technique of deceiving people into giving away confidential information that could be useful to gain unauthorized access to an information system. Even to the most secured system, social engineering is a formidable threat. It is one of the most devastating threats to organizations and businesses. Unlike traditional hacking, social engineering is less or non-technological. It manipulates characteristics of human nature, exploiting people's desire to be kind and helpful. The psychology leverage makes social engineering hard to defend against. This paper presents the identification of factors related to social engineering in the context of armed forces through a review of related literature. Prior works from previous studies are discussed, and factors have been identified based on certain criteria. This study executed a pilot analysis on 30 samples of respondents among Malaysian armed forces personnel. As a result, nine factors are identified that may affect defense against social engineering in the armed forces: Authority, Reciprocation, Commitment and Consistency, Diffusion of Responsibility, Scarcity, Friendliness and Liking, Awareness, Social Proof, and Trust.

Keywords: *Social Engineering, Armed Forces, Security Factors, Information Security*

1. Introduction

Social engineering as means of attack is no longer a new thing. It is a skill of deceiving, to convince people that the social engineer is someone he is not, using influence and persuasion [1]. Some prominent cyberattacks on large organizations used social engineering as an entry point into the organization's systems. Attackers employ a range of tactics that lead a target to disclose sensitive information, including shoulder surfing, dumpster diving, and impersonation; some also involve technological aspects such as vishing, pop-up boxes, and email attachments [2].

Many organizations and individuals have suffered an enormous amount of loss from social engineering attacks since they can lead to privacy violation, financial loss, as well as reputational damage, and potential legal penalties for lost data if an organization is targeted. The military history has recorded various computer incidents which turn out to be happening because of the human factor. For example, in 2008, the Pentagon faced a massive cyber-attack [3]. The incident is dubbed as

* *Corresponding author. nurazean.kl@utm.my*

"the worst breach of U.S military computers in history" or "the most significant breach of U.S. military computers ever" [4]. Personnel allegedly picked a USB flash drive he found in a Department of Defense (DOD) parking lot at a base in the Middle East, unsuspecting that a foreign intelligence agency infects the flash drive with malicious code (malware). He later plugged it into a laptop computer connected to the United States Central Command (CENTCOM) network. The malware then duplicated and uploaded itself to the network and successfully spread and infected other systems, including the military classified systems. Within the CENTCOM network, the malware had established "a digital beachhead from which data could be transferred to servers under foreign control" [5]. The attack has caused the Pentagon 14 months to clean the worm from their network through a military operation called Operation Buckshot Yankee. The malware was later identified as "agent.btz". This social engineering attack is known as "baiting", where the social engineer left a malware-infected storage medium to be found by the victim [6]. The U.S military has then formed U.S Cyber Command in the effort of drawing cyber defense by the military under a single organization [5].

Recognizing the warfare revolution, the Malaysian Armed Forces (MAF) has foreseen that information warfare is a new threat to the nation, as a tool for the enemy to use against the sovereign nation of Malaysia [7]. Preparing the force for this new threat, the MAF had introduced the Fourth Dimension Malaysian Armed Forces (4D MAF) strategy plan in 2008 [8]. The 4D MAF plan aimed to transform the MAF tri-services forces; the Malaysian Army, the Royal Malaysian Navy (RMN), and the Royal Malaysian Air Force (RMAF), into a fully homogeneous, integrated, and unified, even and balanced force, to empower jointness interoperability among the forces. It always has been the MAF's vision to protect the nation and its strategic interest against external aggression; thus, ensuring that the MAF has the necessary assets, resources and capability is part of the 4D MAF objective [9]. The 4D MAF plan highlighted three main attributes: joint force integration and operations, information superiority focusing on network-centric operations (NCO); and multi-dimensional operations in the sub-surface, surface, air and information warfare [10].

This is also a major concern for the National Cyber Security Agency (NACSA), highlighting the seriousness of the necessity for information warfare defense following the worrying increasing incidents about cyberattacks to government agencies' computers, networks, and websites and commercial. As one of the Malaysian government's initiatives to address cyber threats, Malaysia Cyber Security Strategy (MCSS) 2020- 2024 has been launched on 12 October 2020, which outlines strategies to mitigate the evolving cyber threats [11].

Although several measures have been established, protecting organizations against social engineering is quite difficult. Even the greatest technical safeguards are meaningless if an attacker can persuade staff successfully. The reason is simple, there will always be the possibility of a "human factor" no matter what controls are being deployed. Many researchers have investigated means of mitigating and safeguarding against social engineering. However, far too little attention has been paid to the factors influencing the effectiveness of the suggested countermeasures. Hence, this paper aims to discover the factors affecting defense against social

engineering attacks among armed forces personnel and test the reliability of the factors through pilot procedures.

2. Background

Social engineering attacks encompass physical, social, and technical aspects that are used in the various phases of an attack. In general, social engineering attacks took four phases of the cycle to be performed; information gathering, developing relationships, exploitation, and execution [12]. The phases are illustrated in Figure 1.

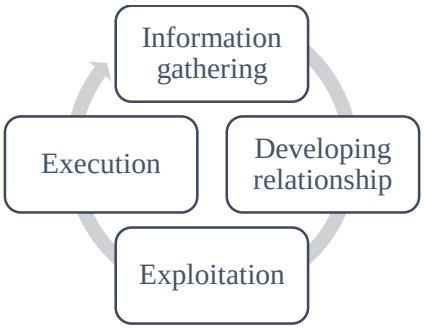

Figure 1: Phases of Social Engineering Attack [12]

In the first phase, the attacker would gather as much information about their target. Once information is successfully collected on a specific target, the attacker may later identify a suitable attack vector that seems familiar or suits the victim's activity and lifestyle [13]. The following phase involves establishing a relationship between the attacker and the victim to determine the level of cooperation and the degree to which the victim may release any potentially sensitive information. At this phase, the attacker may begin with passive reconnaissance, and once the trust has been obtained, a more aggressive active reconnaissance will occur when the trust is established.

The exploitation phase is actively infiltrating the target using both information and relationships. The exploitation could be carried out through casual chats without raising suspicion, such as requesting help to unlock a door, which would allow the attacker access to the organization's facilities. The final phase is when the attacker reaches his ultimate objective, or the attack ends in a way that prevents suspicion.

A number of researchers have suggested various countermeasures strategies against social engineering attacks. For example, organizations are suggested to use a list of core controls to implement and maintain preparedness as countermeasures [12]. In one of the articles published in the SANS Information Security Reading Room, the researcher highlighted the necessity of security policy, education, awareness of threats, and identity management as countermeasures to reduce the impact of an attack [14]. It is also proposed the necessity of insurance protection as cost mitigation to reduce the financial impact to an organization. Another study suggests to include general security culture and risk management as the prevention strategies against social engineering [15].

A number of related studies make general efforts to identify relationships that affect employee's resilience to social engineering attacks. In [16], the study focused on identifying the entities and the relationships between the entities in social engineering attacks. The study has formulated a social engineering-based attack model about the vulnerable entities and the safeguards methods against social engineering.

Another study discussed factors that influence employees' resilience to social engineering attacks at both governance and individual level [17]. In the same study, the role of national culture is also evaluated in terms of its influence on relationships. Based on the result of the research, six factors have been identified which significantly affecting employee's resilience to social engineering attacks:

a. Trust: Employees who demonstrated a substantial trust are easier to be conned, thus less resilient to social engineering attacks.
b. Risky behaviors: Employees who acted without taking into consideration the consequences of their actions are often targeted by a social engineer, thus less resilient.
c. General information security awareness: Employees who familiar with threats and have knowledge of the consequences of a lack of information security are less likely to fall victim to social engineering. Thus, are more resilient to social engineering attack.
d. Security and computer knowledge: Employees who are trained with formal security and computer training are more resilient to social engineering attacks due to solid experience with computer technologies.
e. Intention: Employees who exhibit obedience to procedures and policies and strongly against compromising them are more resilient to social engineering attacks.
f. Target-related information: Social engineers who made thorough preparation and composed his attack with a good amount of information specifically about his target are most likely to get employees of the target organization to fall victim to the attack.

In addition to governance and individual factor, another study discussed the correlation between culture and employee's resilience to social engineering attacks [17]. The findings demonstrate that national culture significantly affects behavioral information security and drivers of employees' social engineering behaviors.

Other researchers are investigating the social engineering field in terms of factors affecting the defense against social engineering. A recent study revealed that leadership and the tendency towards risky behavior could be viewed as major elements impacting security awareness, leading to resistance against social engineering attacks [18]. A summary of previous studies is shown in Table 1, where the key findings are used as a basis in the context of armed forces.

Table 1. Key Findings in Related Social Engineering Studies

No.	Key Findings	Respondents	Methodology	References
1.	The study emphasized how badly an attack could damage the organization. Hence, the defense method is tabled briefly. Besides paying attention to the people, the study also highlighted technological approaches instrumental in defending against social engineering attacks.	Employees from various organizations and industries	Qualitative	[2]
2.	The study highlighted that vulnerable entities may allow or motivate the attacker to perform the attack. Most internet users have faced different types of social engineering attacks during their online time. It is found that the majority of the people do not understand or aware of the threat of social engineering and its consequences.	Employees from various organizations and industries	Quantitative	[16]
3.	The study revealed that employees' security behavior contributes the most to their level of resilience to social engineering attacks. The author has thoroughly identified the factors influencing employees' resilience to social engineering, divided into two main levels, governance and individual. In addition, the effect of culture in shaping employees' security behavior is also investigated. With proper actions taken, employees' resilience to social engineering can be ensured or improved.	Employees (high-level executives as CISOs, Security Officers, CEOs, CIOs, and IT managers)	Mixed-methods	[17]
4.	The study examined both individual and organizational factors toward risky behavior that are influencing information security awareness of employees. The study confirmed that employees' awareness of information security leads to intention to resist social engineering attacks. Also, the study indicated that leadership and the tendency towards risky behavior had influenced information security awareness. Organizations should therefore consider the tendency toward risky	Employees from various organizations and industries	Quantitative	[18]

* *Corresponding author. nurazean.kl@utm.my*

No.	Key Findings	Respondents	Methodology	References
	behavior, training, and workshops related to awareness-raising activities.			
5.	The study suggested that people's perceptions about software to mitigate information security threats have resulted in their reckless behavior, increasing the organization's vulnerability. To formulate the information security guidelines within organizations, perceived severity and perceived susceptibility are important key elements. It is also identified that users' satisfaction with the organization affected their safe behavior.	Employees from various organizations and industries	Quantitative	[19]
6.	This study proposed an ontological model for Social Engineering attack based on the analysis of existing definitions and taxonomies. The model represented six entities: target, medium, goal, technique, social engineer, and compliance.	N/A	N/A	[20]
7.	The study reviewed the ontological model proposed by the same authors in order to further define the social engineering domain. Based on Kevin Mitnick's social engineering attack cycle, a social engineering attack framework is proposed. The attack framework includes specific steps for identifying components as well as details on all other parts of an attack. The framework and the ontological model can be employed to develop scenarios of social engineering attacks.	N/A	N/A	[21]

3. Proposed Conceptual Model

As illustrated in Figure 2, the conceptual model was developed based on theoretical model factors affecting employees' resilience to social engineering attacks by [17]. Nine factors are shortlisted to be included in the proposed model after inclusion and exclusion are completed. The factors affecting defense against social engineering comprise Authority, Reciprocation, Commitment and Consistency, Diffusion of Responsibility, Scarcity, Friendliness or Liking, Awareness, Social Proof, and Trust. The selection of factors is based on the frequency of the papers appearing in the literature and their relevancy in the environment of the armed forces.

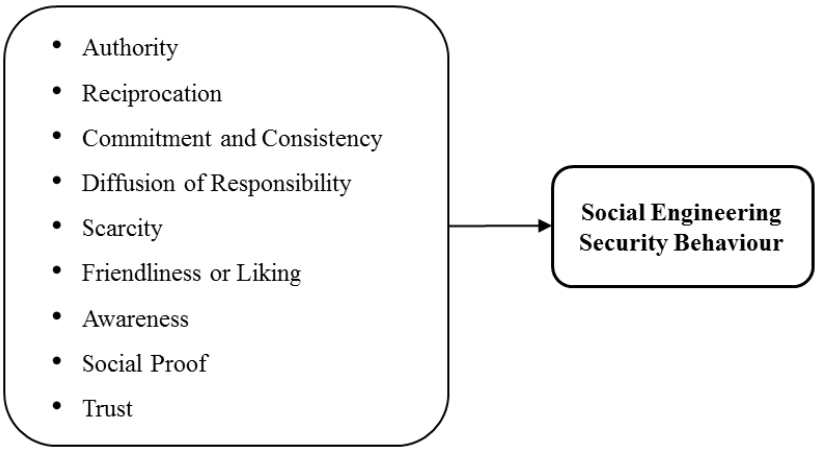

Figure 2: Proposed Conceptual Model for Identifying Factors Affecting Defence Against Social Engineering in the Armed Forces

Authority has the highest frequency among the other factors [22,23]. Orders or requests received from someone with higher authority are usually easier to be accepted by the victim without further question. In the military culture, personnel with higher ranks usually comes with higher authority.

Reciprocity is an act of repaying kindness for a favor [20,21]. In terms of social engineering, people are more willing to comply with requests by a requester who had treated them favorably. It is because they feel grateful and indebted for the good treatment.

Commitment and consistency is a "mental shortcut" people used in daily life to simplify decision-making [23]. It made lives easier by reducing the number of things to think about. A person will just make a single decision and then use this decision as a reference for subsequent related choices. In a real scenario in social engineering, the social engineer will first commit to his victim person or organization.

Diffusion of responsibility is when people feel that the responsibility is dispersed among many others, thus reducing the burden on their shoulders [24]. Security-wise, in the event of a threat, a person might feel that his responsibility for taking action in protecting the information is lessened when other people of the same position or responsibility are present.

** Corresponding author. nurazean.kl@utm.my*

Scarcity is a principle that is based on the future unavailability of opportunities, or anything, even if it is not needed [20,23]. Often things will seem more valuable when their availability is limited or nearing to scarce. People will be motivated by the idea of losing something than gaining something of equal value.

Regarding Friendliness and Liking, people are prone to influence and cooperate with people they like [21]. A social engineer often uses it to craft his attack, as people are more likely to comply with requests from the person he likes.

Education and training of employees' awareness to threat is the key to security [16]. They need to be taught what threat they might face. The most important thing is employees must be trained to identify an attack. In the event of an attack, they could respond to it accordingly to neutralize it or minimize the impact on the organization.

Social Proof is the tendency of someone to take behavioral cues from the people around them. People pay less consideration to other factors, including security, when doing something that seems socially correct.

Trust can be manipulated by persuading the victim to have faith in the social engineer that he's a good person. People showing more trust towards another party are more likely to fall victim to social engineering, thus decreasing social engineering defense effort.

4. Methodology

This study executed a pilot study analysis procedure involving quantitative data to test the reliability of the factors being proposed. The quantitative approach is based on the measurement of quantity or amount. This pilot study consisted of two phases as described in [25]; (1) Expert-Driven Pretests and (2) Respondent-Driven Pretests.

The first phase is to get an expert review for opinions and comments on the questionnaire's content. The experts are asked to review the entire survey and rate the items on a Likert scale. Their judgment is required to see how well each questionnaire items truly reflects the factors that this study intends to measure.

The second phase is distributing the survey to a small subsample of the sample population. In this study, the survey has been distributed to 30 respondents among MAF personnel.

5. Pilot Study Analysis

In the first phase, three experts were invited to review the questionnaire, which included 30 indicators for all nine factors. The profiles of expert reviewers are shown in Table 2.

Continuing from the first phase, a pilot survey was conducted and 30 respondents from MAF personnel were requested to answer the survey questionnaire. Google Form was used to build and distribute the survey.

Table 2. Expert Reviewer Profile

Expert Reviewer	Position	Institution
1	Head of Cyber Defense Branch	DISD, MAF
2	Director of IT	RMN HQ
3	Senior Lecturer	UTM

Upon receiving feedback from all respondents, an analysis using a statistical tool software called SmartPLS is used in order to examine the indicators and factors' consistency reliability by obtaining the Outer Loading value for indicators and Cronbach Alpha (α) value for factors.

After undergoing some indicator reductions, followed by a reduction of factors, the analysis was then repeated to determine the most reliable factors and indicators that contribute to Social Engineering Security Behavior. The finalized analysis result of this pilot study is as shown in Table 3.

Table 3. Pilot Study Result

Factors	Items	Cronbach Alpha (α) Values	Outer Loading Value	Reliability
Social Engineering Security Behaviour		0.815		Good
	DV1		0.783	
	DV2		0.934	
	DV3		0.840	
Authority		0.610		Acceptable
	AU2		0.788	
	AU3		0.651	
	AU4		0.766	
Commitment and Consistency		0.667		Acceptable
	CC1		0.884	
	CC2		0.847	
Diffusion of Responsibility		0.848		Good
	DR1		0.918	
	DR2		0.809	
	DR3		0.880	
	DR4		0.695	
Awareness		0.866		Good
	AW2		0.938	
	AW3		0.940	
Trust		0.809		Good
	T1		0.828	
	T2		0.815	
	T3		0.890	

As a general rule of thumb, for a factor to be considered reliable, its value of Cronbach Alpha (α) must be α>0.7 [26]. In this study, the criteria of Cronbach Alpha (α) for establishing internal consistency reliability used is as suggested in [27] and [28], that is Excellent (α>0.9), Good (0.7<α<0.9), Acceptable (0.6<α<0.7), Poor (0.5<α<0.6), Unacceptable (α<0.5). Accordingly, the results show that the items and factors are considered reliable to be tested in the next stage of our study.

6. Conclusion

The results from this pilot study should be viewed as an indication for further research. However, the results were interesting and indicate that the respondents find that *Authority*, *Commitment and Consistency*, *Diffusion of Responsibility*, *Awareness*, and *Trust* could be the most reliable factors and indicators that contribute to Social Engineering Security Behavior. The results also should give us an early evaluation of employees' ability to prevent social engineering attacks in the environment of the armed forces. Knowing which factors affecting the defense to social engineering attacks will allow the organization to detect or even foretell which kinds of attacks will more likely to succeed in a specific personnel group. This will also assist in the development of appropriate countermeasure steps such as guidelines, team building and customized high-level awareness training.

Acknowledgments

We would like to thank Universiti Teknologi Malaysia, Ministry of Education Malaysia and Malaysian Armed Forces.

References

[1] Kevin D. Mitnick, William L. Simon. The Art of Deception: Controlling the Human Element of Security | Wiley [Internet]. John Wiley & Sons; 2011 [cited 2021 Jul 9]. Available from: https://www.wiley.com/en-us/The+Art+of+Deception%3A+Controlling+the+Human+Element+of+Security-p-9780764538391

[2] Janczewski LJ, Fu L. Social engineering-based attacks: Model and New Zealand perspective. Proc Int Multiconference Comput Sci Inf Technol IMCSIT 2010. IEEE Computer Society; 2010. p. 847–53.

[3] Bogdanoski M, Petreski D. Cyber Terrorism-Global Security Threat. Int Sci Defence, Secur Peace J. 2013;13:59–73.

[4] Geers K, Kindlund D, Moran N, Rachwald R. Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks [Internet]. 2014. Available from: www.fireeye.com

[5] Lynn WJ. Defending a New Domain: The Pentagon's Cyberstrategy. Foreign Aff. 2010;89:97–108.

[6] Krombholz K, Hobel H, Huber M, Weippl E. Advanced social engineering attacks. J Inf Secur Appl. Elsevier Ltd; 2015;22:113–22.

[7] The Straits Times. Malaysia's armed forces confirms cyber-attack on network,

SE Asia News & Top Stories [Internet]. 2020 [cited 2021 Jul 9]. Available from: https://www.straitstimes.com/asia/se-asia/malaysias-armed-forces-confirms-cyber-attack-on-network
[8] Zainal AA. Perutusan khas Panglima AngkatanTentera Sempena Jubli Intan ATM. Perajurit 16. Syed Hussain Publications Sdn Bhd, Kuala Lumpur; 2009. p. 2–5.
[9] Azizan. Top Brass Interview: General Tan Sri Azizan Ariffin, Chief of Air Force, RMAF. Asian Def J. Syed Hussain Publications Sdn Bhd, Kuala Lumpur; 2009. p. 11–4.
[10] Harun N. Komitmen kami, keyakinan anda: ATM bersedia menghadapi cabaran baru. Perajurit. Syed Hussain Publications Sdn Bhd, Kuala Lumpur; 2008. p. 21–5.
[11] Bernama. Govt launches RM1.8b Malaysia Cyber Security Strategy | Malaysia | Malay Mail. Malay Mail [Internet]. 2020 [cited 2021 Jul 9]; Available from: https://www.malaymail.com/news/malaysia/2020/10/12/govt-launches-rm1.8b-malaysia-cyber-security-strategy/1912008
[12] Allen M. Social Engineering: A Means to Violate a Computer System. SANS Inf Secur Read Room. 2006;
[13] Hidayah Zulkiffli SN, Ahmad Zawawi MN, Rahim FA. Passive and Active Reconnaissance: A Social Engineering Case Study. 2020 8th Int Conf Inf Technol Multimedia, ICIMU 2020. 2020;138–43.
[14] Radha Gulati. The Threat of Social Engineering and Your Defense Against It. SANS Inf Secur Read Room. 2003;
[15] Veronika P. Social Engineering risk classification and major prevention strategies. 2013.
[16] Chitrey A, Singh D, Bag M, Singh V. A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model. Int J Inf Netw Secur. 2012;1:45–53.
[17] Flores WR. Shaping Information Security Behaviors Related to Social Engineering Attacks. [Stockholm, Sweden]: Royal Institute of Technology; 2016.
[18] Grassegger T, Nedbal D. The role of employees' information security awareness on the intention to resist social engineering. CENTERIS - Int Conf Enterp Inf Syst / ProjMAN - Int Conf Proj Manag / HCist - Int Conf Heal Soc Care Inf Syst Technol 2020. Elsevier B.V.; 2021. p. 59–66.
[19] Klein RH, Luciano EM. What Influences Information Security Behavior? A Study with Brazilian Users. - J Inf Syst Technol Manag. 2016;13:479–96.
[20] Mouton F, Leenen L, Malan M, Venter H. Towards an Ontological Model Defining the Social Engineering Domain. 11th IFIP Int Conf Hum Choice Comput [Internet]. Turku, Finland; 2014 [cited 2021 Jul 9]. p. 266–79. Available from: https://hal.inria.fr/hal-01383064
[21] Mouton F, Malan MM, Leenen L, Venter HS. Social engineering attack framework. 2014 Inf Secur South Africa - Proc ISSA 2014 Conf. Institute of Electrical and Electronics Engineers Inc.; 2014.
[22] Kronberg B, Svanlund J, Jeppsson H. Social Engineering: A study in awareness and measures. 2015.
[23] Quiel S. Social Engineering in the Context of Cialdini's Psychology of Persuasion and Personality Traits [Internet]. [Hamburg, Germany]: Hamburg University of Technology; 2013 [cited 2021 Jul 9]. Available from:

https://www.sva.tuhh.de/
[24] Bezuidenhout M, Mouton F, Venter HS. Social engineering attack detection model: SEADM. Proc 2010 Inf Secur South Africa Conf ISSA 2010. 2010.
[25] Ruel E, Wagner WE, Gillespie BJ. Pretesting and Pilot Testing. Pract Surv Res Theory Appl. SAGE Publications, Inc; 2016. p. 101–19.
[26] Hair JF, Sarstedt M, Hopkins L, Kuppelwieser VG. Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. Eur Bus Rev. Emerald Group Publishing Ltd.; 2014;26:106–21.
[27] Manerikar V, Manerikar S. "Cronbach's alpha," A Peer Reviewed Research Journal. aWEshkar. 2015;XIX:117–9.
[28] George D, Paul Mallery with. SPSS for Windows Step by Step A Simple Guide and Reference Fourth Edition (11.0 update) Answers to Selected Exercises. Allyn and Bacon; 2003.