International Journal of Computer Applications Technology and Research
Volume 6–Issue 1, 42-50, 2017, ISSN:-2319–8656

The Current State of Phishing Attacks against Saudi Arabia University Students

Bushra Mohamed Elamin Elnaim
Department of Computer Science and Information
Sattam bin Abdulaziz University
Al Sulail, Kingdom of Saudi Arabia

Hayder Abood S.Wsmi.Al-Lami
Department of Computer Science and Information
Sattam bin Abdulaziz University
Al Sulail, Kingdom of Saudi Arabia

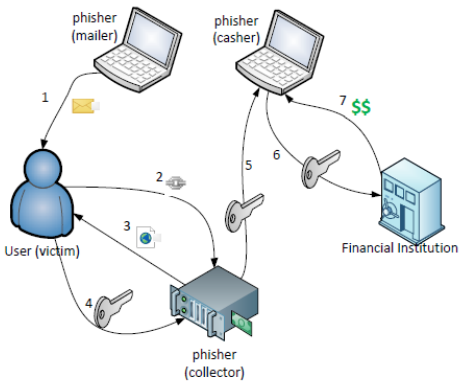
Abstract:

Research into phishing and social engineering is a very interesting area since a significant number of attacks are conducted with the help of social engineering and phishing as the main vector to either obtain credentials or trick the user into executing a malware infected file. The goal of our research was to examine the students' familiarity with threats in the form of phishing attacks conducted via the Internet. A questionnaire was conducted to determine the students' ability to recognize phishing attacks and if they know how to protect themselves. The motivation behind this research is to explore the Saudian Student population's self assessment in regard to phishing attacks and to assess their capability on a limited data set for purpose of obtaining a baseline for future research.

Keywords: phishing attack; Saudi Arabia student; social engineering; Phishing Attacks in KSA universities; Types of phishing attacks.

1. INTRODUCTION

Phishing is a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion [1]. The word "phishing" appeared around 1995, when Internet scammers were using email lures to "fish" for passwords and financial information from the sea of Internet users; "ph" is a common hacker replacement of "f", which comes from the original form of hacking, "phreaking" on telephone switches during 1960s [2]. Early phishers copied the code from the AOL website and crafted pages that looked like they were a part of AOL, and sent spoofed emails or instant messages with a link to this fake web page, asking potential victims to reveal their passwords [3]. A complete phishing attack involves three roles of phishers. Firstly, mailers send out a large number of fraudulent emails (usually through botnets), which direct users to fraudulent websites. Secondly, collectors set up fraudulent websites (usually hosted on compromised machines), which actively prompt users to provide confidential information. Finally, cashers use the confidential information to achieve a pay-out. Monetary exchanges often occur between those phishers. Show Figure(1):



Figure(1): Phishing Information Flow

2. LITERATURE REVIEW

2.1 Types of Phishing Attacks

Numerous different types of phishing attacks have now been identified. Some of the more prevalent are listed below:

2.1.1 Deceptive Phishing

The term "phishing" originally referred to account theft using instant messaging but the most common broadcast method today is a deceptive email message. Messages about the need to verify account information, system failure requiring users to re-enter their information, fictitious account charges, undesirable account changes, new free services requiring quick action, and many other scams are broadcast to a wide

group of recipients with the hope that the unwary will respond by clicking a link to or signing onto a bogus site where their confidential information can be collected.[4]

2.1.2 **Malware Phishing**

Phishing scams involving malware require it to be run on the user's computer. The malware is usually attached to the email sent to the user by the phishers. Once you click on the link, the malware will start functioning. Sometimes, the malware may also be attached to downloadable files.

Phishers take advantage of the vulnerability of web security services to gain sensitive information which is used for fraudulent purposes. This is why it's always a good idea to learn about the various phishing techniques, including phishing with Trojans and Spyware.[5]

2.1.2 Key loggers and Screen loggers

Key loggers and screen loggers are varieties of malware that track input from the keyboard and send relevant information to the hacker via the Internet. They can embed themselves into the user's browsers as small utility programs.[6]

2.1.4 Session hijacking attack

The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token.

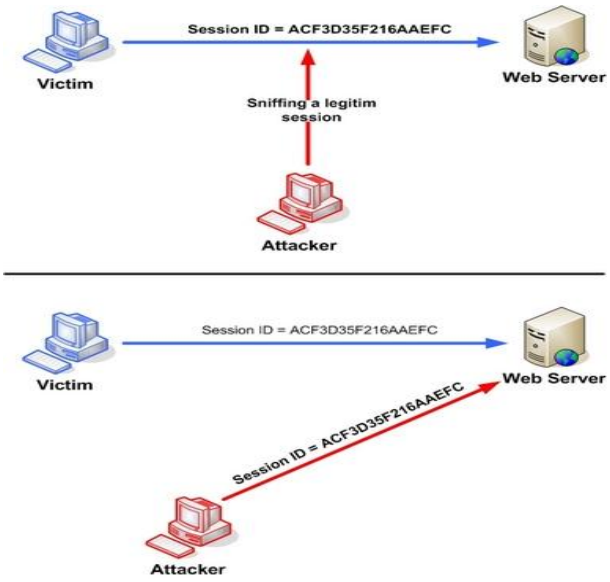
Because http communication uses many different TCP connections, the web server needs a method to recognize every user's connections. The most useful method depends on a token that the Web Server sends to the client browser after a successful client authentication. A session token is normally composed of a string of variable width and it could be used in different ways, like in the URL, in the header of the http requisition as a cookie, in other parts of the header of the http request, or yet in the body of the http requisition.

The Session Hijacking attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server.

The session token could be compromised in different ways; the most common are:[7]

- Predictable session token;
- Session Sniffing;
- Client-side attacks (XSS, malicious JavaScript Codes, Trojans, etc);

As an example the following figure:



Figure(2): Session Sniffing

In figure(2) , as we can see, first the attacker uses a sniffer to capture a valid token session called "Session ID", then he uses the valid token session to gain unauthorized access to the Web Server.

2.1.5 Trojan Virus

A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems. Once activated, Trojans can enable cyber-criminals to spy on you, steal your sensitive data, and gain backdoor access to your system. These actions can include:

- Deleting data
- Blocking data
- Modifying data
- Copying data
- Disrupting the performance of computers or computer networks

Unlike computer viruses and worms , Trojans are not able to self-replicate.[8]

2.1.6 DNS Poisoning

DNS poisoning is a method which gives the impression that hackers took control of some known sites or not. DNS is the protocol which connects domain name and IP address for any site in the world has one or more IP addresses. When we write in the browser "google.com" our computer has three options for finding IP address or addresses for "google.com".
1.Prima option-hosts file in C :/ windows / system32 / drivers

/ etc / hosts
2.A second option - private DNS (server, router)
3.A third option - public DNS servers (OpenDNS, Google DNS).
Wherever you find the IP address for "google.com" our computer stops and no longer see the other variants. For example, if the IP address found for "google.com" in the hosts file, it does not go and that public private DNS to confirm the validity of those addresses.
Thus we can to fool the PC, we can tell him anything, he will believe anything found in the hosts file.[9]

2.1.7 **System Reconfiguration Attacks**
Modify settings on a user's PC for malicious purposes. For example: URLs in a favorites file might be modified to direct users to look alike websites. For example: a bank website URL may be changed from "bankofabc.com" to "bancofabc.com".**[10]**

2.1.8 Data Theft

Data theft is the act of stealing computer-based information from an unknowing victim with the intent of compromising privacy or obtaining confidential information. Data theft is increasingly a problem for individual computer users, as well as big corporate firms.

There is more than one way to steal data. Some popular methods are listed below:[11]

- E-commerce: You should make sure that your data is safe from prying eyes when you sell or buy things on the Web. Carelessness can lead to leaking your private account information.
- Password cracking: Intruders can access your machine and get valuable data if it is not password-protected or its password can be easily decoded (weak password).
- Eavesdropping: Data sent on insecure lines can be wiretapped and recorded. If no encryption mechanism is used, there is a good chance of losing your password and other private information to the eavesdropper.
- Laptop theft: Increasingly incidents of laptop theft from corporate firms occur with the valuable information stored in the laptop being sold to competitors. Carelessness and lack of laptop data encryption can lead to major losses for the firm**.**

2.1.8 DNS-Based Phishing Attacks
Domain Name System (DNS)-based **phishing** or hosts file modification is called Pharming. The requests for URLs or name service return a bogus address and subsequent communications are directed to a fake site when the hackers tamper a company's host files or domain name. As a result, users remain unaware about the fraud website controlled by hackers.[12]

2.1.9 Man**-in-the-Middle Phishing**:

Abbreviated as **MITMA**, a **man-in-the-middle attack** is an attack where a user gets between the sender and receiver of information and sniffs any information being sent. In some cases, users may be sending unencrypted data, which means the man-in-the-middle (MITM) can obtain any unencrypted information. In other cases, a user may be able to obtain information from the attack, but have to unencrypted the information before it can be read. In the picture below is an example of how a man-in-the-middle attack works. The attacker intercepts some or all traffic coming from the computer, collects the data, and then forwards it to the destination the user was originally intending to visit. Shown in figure (3):[13]

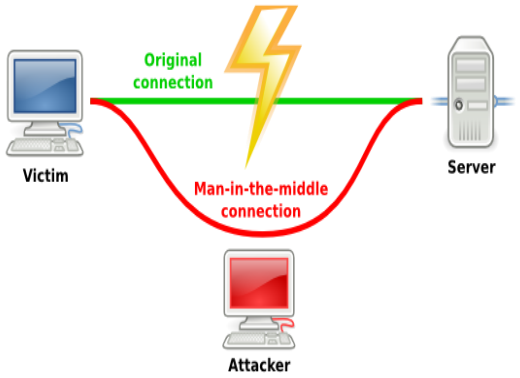


Figure (3): shows Man in Middle Attack

2.1.10 SEO poisoning (search poisoning)

SEO poisoning, also known as search poisoning, is an attack method in which cybercriminals create malicious websites and use search engine optimization tactics to make them show up prominently in search results. The sites are associated with terms that large numbers of people are likely to be using in searches at any given time, such as phrases related to holidays, news items and viral videos. According to Web sense Security Labs, up to a quarter of the first page of search results for trending topics are linked to malicious websites.

The attackers create websites with names and descriptions associated with popular or trending topics. For example, in the weeks leading up to Halloween, the attackers might launch sites offering free templates for Halloween costumes; in the weeks or months leading up to Christmas, they might launch holiday recipe sites. The sites might be devoid of relevant content or might feature content stolen from valid sites. The real purpose, however, is to infect visitors with malware or fraudulently access sensitive information to be used

for identity theft. Malware on the site may coopt the visitor's computer for a botnet or install a Trojan horse to steal login information. Another ploy is to present the user with a product that they think they are purchasing to access their credit card details. [14]

2.2 Related Works

There are different studies which focus on Phishing attacks in KSA:

In [15] research was conducted to introduce and analyze a high level (a country-based) anti-phishing countermeasure implemented in Saudi Arabia. An investigation was carried out to examine whether this countermeasure is effective against phishing scenarios. The countermeasure is considered effective when Phishing websites are reached by users who surf the Internet inside Saudi Arabia whereas it is ineffective when the websites are reached by users who surf the Internet from outside Saudi Arabia.

In [16] study, discuss and propose the phishing attack stages and types, technologies for detection of phishing web pages, and conclude with some important recommendations for preventing phishing for both consumer and company that can be taken to reduce vulnerabilities to phishing attacks.

In [17] the purpose of this paper is to report the findings of the study commissioned by the Communications and Information Technology Commission to ascertain the magnitude of spam in the Kingdom of Saudi Arabia and formulate a comprehensive multi-pronged solution for handling spam in Saudi Arabia based upon best international practices, current situation and national requirements. It is only focus on determining the current state of spam in KSA, focusing on obtaining a good understanding of the nature and prevalence of spam within Saudi Arabia. This information will then form the basis upon which the anti-spam national strategy framework will be based.

In [18] This paper discusses the stand of Saudi Arabian government against cyber crime and its IT act. It analyzes the cybercrime in the Kingdom and the anti-cyber crime law. It shows that Saudi Arabia was ranked first as the most vulnerable of the Gulf countries to fall victim to cyber-crimes, such as website hacking. It shows that most of the people in KSA know about cyber crime but very less is aware of the associated legislation to combat these crimes. Therefore, in KSA it has been clear how computer crimes can affect people live especially for those financial crimes. Although, the information security is increased but also the unauthorized access for example were dramatically increased. It also concludes that knowing the laws of computer crimes should be considered the first solution to reduce them.

2.3 Examples of Phishing Attacks in KSA Universities

Due to the frequent use by Saudi students and professors of computer networks for learning and teaching, universities have a large degree of exposure to cyber attacks.

"At the end of May 2015, a hacker in Saudi Arabia claimed to have hacked and stolen information from a Saudi university's network," he explains, "including the personal details, academic results and schedules of 4,000 university students."[19]

In 2012, The Official Website of **King Saud University (KSU)** , is a public university located in Riyadh, Saudi Arabia hacked by some unknown Hacker. Database of 812 Users hacked from http://printpress.ksu.edu.sa/ and dumped on Internet by Hacker on a file sharing site including Mail address list, mobile phones and passwords.[20]. See figure (4):

	A	B	C	D	E
1	Memail	mmobile	mname	mpassword	musername
2	almas-59@hotmail.com	NULL	*******	123098	*******
3	almas-59@hotmail.com	NULL	**********	123098	**********
4	NULL	NULL	abdulhak		NULL
5	HAKIM_M4@YAHOO.COM	NULL	ABDULHAKIM	1091962	HAKIM99
6	alsayed.abdulhameed@hotmail.com	NULL	abdulhameed	1200	abdulhameed
7	ahdswd@gmail.com	504131034	Abdulhameed Al-Sawadi		ahdswd
8	aajabbar@gmail.com	NULL	Abdulhamid Alabduljabbar		ajabbar
9	aalhargan@gmail.com	NULL	Abdulhamid Alhargan		aalhargan
10	aayr1978@gmail.com	599291990	abdulkarem	0	abdulkarem
11	mustaf_abdulkarim@yahoo.ca	NULL	Abdulkarim		karimmustaf
12	ahowaish@kfu.edu.sa	566776060	Abdulkarim Alhowaish		alhowaish
13	abdullajmb@hotmail.com	9.68E+11	abdulla		
14	hamadeana@maktoob.com	734414933	abdulla ghalib		hamadeana
15	arf1430@hotmail.com	NULL	abdullah	30153015	abdullah
16	gubbad55@hotmail.com	507097542	Abdullah Ahmed		gubbad55
17	aanazi@hotmail.com	504474788	Abdullah Al-Anazi	123456	aanazi
18	abdullah_aldhuwaihi@yahoo.com	NULL	Abdullah Aldhuwaihi		abdullah_aldhuwaih
19	a9algarni@gmail.com	505760362	abdullah ali algarni	760362	al_garni
20	gahtany@hotmail.com	NULL	Abdullah Al-Kahtani		gahtani
21	muhaidib@ksu.edu.sa	NULL	abdullah almhaidib		muhaidib
22	aalomari_sa@yahoo.com	NULL	abdullah alomari		binjeddah
23	asalman@ksu.edu.sa	NULL	abdullah alsalman		asalman
24	aalshalan@yahoo.com	NULL	Abdullah Alshalan		aalshalan
25	abedbody_626_@hotmail.com	NULL	abdullah baddah	1402111	abdullah.b

Figure (4): King Saud University database hacked

3. MAIN STUDY

3.1 Participants

The Questionnaire was administrated to fifty (50) participants, who were undergraduate students, from Prince Sattam Bin A bdulaziz University. Age ranged from 18 to 22 with the gender 40 male and 10 female. Each participants took part in the survey on a fully voluntary basis. A summary of the demographics of the participants in the main study is shown in table (1).

Table (1): Participant Demographics in The Main Study.

Characteristics	Total
Sample Size	50
Gender	
Male	40
Female	10
Age Range (From 18 To 22)	50
Average Hours Per Week on The Internet	
0—5	3
6—10	5
11—15	5
16—20	9
20 +	28

3.2 Procedure

The questionnaire was handled out to participants in-person by the researcher. First, the nature of the research was explained to each participant individually. They were told that they were free to withdraw from the study at any time without having to give a reason for withdrawing. Then participants were asked to complete the questionnaire, they were asked whether or not they know what the term " Phishing Attack" means, and if they know how to protect against phishing attack, they were asked also if they know the difference between http and https protocols, if they were familiar with the term " Social Engineering", if they were check the URL after the opening new web site link. The individual particpciant was given 15 min to complete the questionnaire. After completing the questionnaire, participants were thanked for their valuable time and effort in taking part in the study.

3.3 Results

We collected 50 valid responses and our sample consisted of students from five different scientific fields of study: Computer science department, business management, Arabic, Islamic studies, and mathematic department. As shown in table (2) and figure (5) which were part of the Prince Sattam bin Abdulaziz University.

Table (2): Show five different scientific fields of study

	Frequency	*Percent*	*Valid Percent*	*Cumulative Percent*
Computer	13	26.0	26.0	26.0
Math.	7	14.0	14.0	40.0
Management	10	20.0	20.0	60.0
Arabic	10	20.0	20.0	80.0
Islamic	10	20.0	20.0	100.0
Total	50	100.0	100.0	

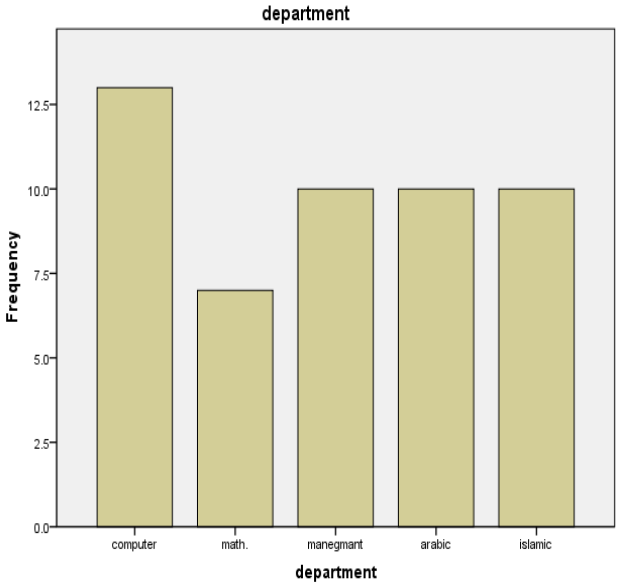


Figure (5) : Frequency of five different department of study

Most of our test subjects, 58.0% stated that they were took 21+ hours per week of internet usage, while 42% were took ≤ 20 hours per week of internet usage as shown in Table (3) and figure (6).

Table (3): The average hours per week of internet experience

Average Hours	Frequency	Percent	Valid Percent	Cumulative Percent
0-5	3	6.0	6.0	6.0
6-10	3	6.0	6.0	12.0
11-15	4	8.0	8.0	20.0
16-20	11	22.0	22.0	42.0
+21	29	58.0	58.0	100.0
Total	50	100.0	100.0	

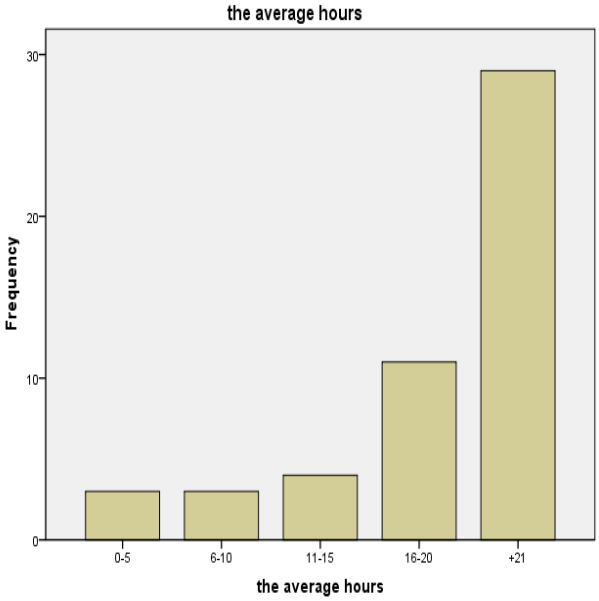


Figure (6): The Average hours per week of internet experience

Table (4) and figure (7) shows the students answer that if they were familiar with the term "Phishing Attack" or not, 50% answered that they were familiar with the term phishing attack and most of them in computer science department, while 50% were not familiar with this term.

Table (4): Student's familiarity with the term Phishing Attack

Answer		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	25	50.0	50.0	50.0
	no	25	50.0	50.0	100.0
	Total	50	100.0	100.0	

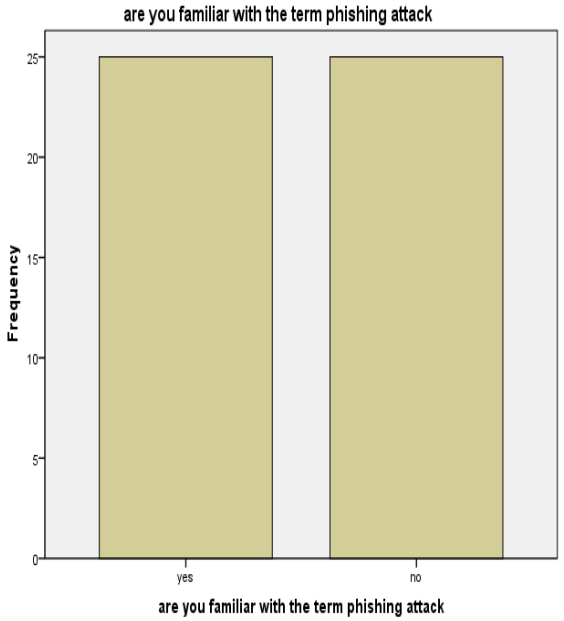


Figure (7): Student's familiarity with the term Phishing Attack

Table (5) and figure (8) shows the students answer that if they know how to protect themselves against phishing attack, 62% were not know how to protect themselves against phishing attacks, while 38% were know.

Table (5): students that were know how to protect themselves against phishing attack

Answer		*Frequency*	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	yes	19	38.0	38.0	38.0
	no	31	62.0	62.0	100.0
	Total	50	100.0	100.0	

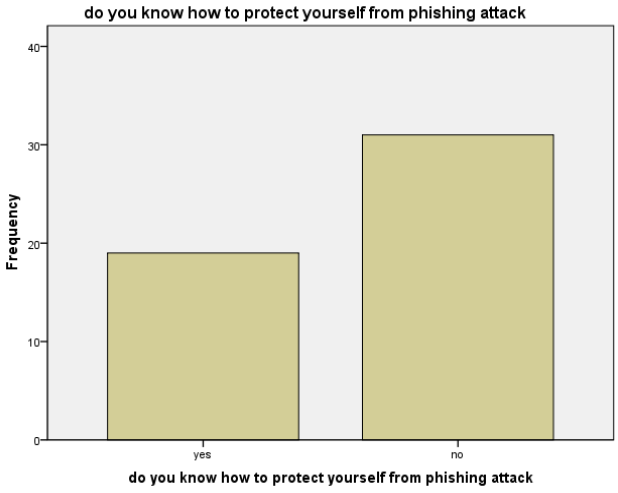


Figure (8): students that were know how to protect themselves against phishing attack

Table (6) and figure (9) shows the students answer that if they were know the difference between http and https protocols, 78% were not know the difference between http and https protocols , while 22% were know.

Table (6): students that were know the difference between http and https protocols

Answer		Frequency	Percent	Valid Percent	Cumulative Percent
	Yes	11	22.0	22.0	22.0
	No	39	78.0	78.0	100.0
	Total	50	100.0	100.0	

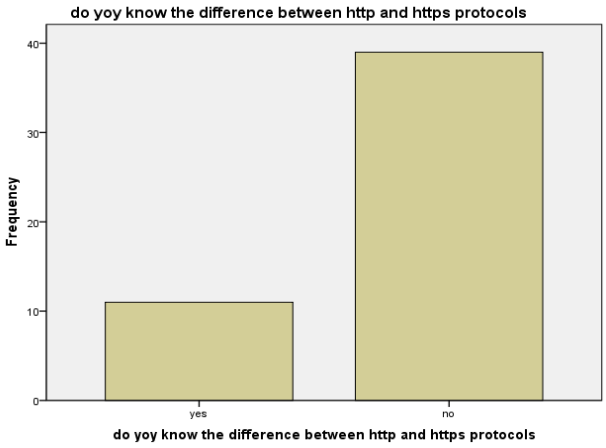


Figure (9): students that were know the difference between http and https protocols

Table (7) and figure (10) shows the students answer that if they were familiar with the term " Social Engineering" or not, 72% were not familiar with the term "social engineering", while 28% were familiar with the term" social engineering".

Table (7): students that were familiar with the term social engineering

Answer		*Frequency*	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	yes	14	28.0	28.0	28.0
	no	36	72.0	72.0	100.0
	Total	50	100.0	100.0	

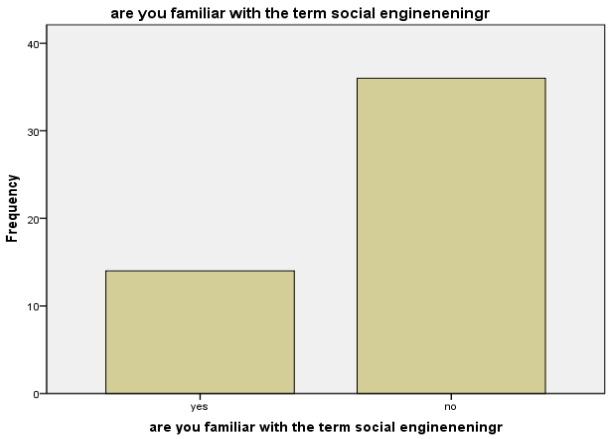


Figure (10): students that were familiar with the term social engineering

Table (8) and figure (11) shows the students answer that if they check the URL after the opening new website link or not, 82% were not check the URL after the opening new website link, 18% check the URL after the opening new website link.

Table (8): students that were check the URL after the opening new website link

Answer		*Frequency*	*Percent*	*Valid Percent*	*Cumulative Percent*
Valid	yes	9	18.0	18.0	18.0
	no	41	82.0	82.0	100.0
	Total	50	100.0	100.0	

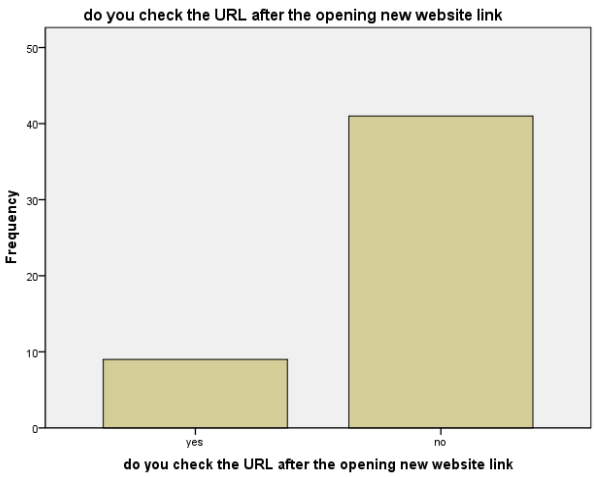


Figure (11): students that were check the URL after the opening new website link

4. CONCLUSION

Some of the interesting results our researches are:

- 58.0% stated that they were took 21+ hours per week of internet usage, while 42% were took ≤ 20 hours per week of internet usage.
- 50% answered that they were familiar with the term phishing attack and most of them in computer science department, while 50% were not familiar with this term.
- 62% were not know how to protect themselves against phishing attacks, while 38% were know.
- 78% were not know the difference between http and https protocols , while 22% were know.
- 72% were not familiar with the term "social engineering", while 28% were familiar with the term" social engineering".
- 82% were not check the URL after the opening new website link, 18% check the URL after the opening new website link.

5. LIMITATIONS

- The study was only conducted on the College of Science and Humanity Studies At Sulail.
- The study was conducted on a student between 18 and 22 years old.
- Students were not given training on phishing attack.

6. RECOMMENDATIONS

Educating saudian students on phishing techniques is an important aspect of internet security, if students were educated about phishing, it can help them understand the methods used to differentiate whether a website is a illegitimate site or a phishing site.

7. ACKNOWLEDGMENTS

Our thanks to the Staff of the College of Science and Humanity Studies At Sulail, Prince Sattam bin abdulaziz university for their contributions and comments.

8. REFERENCES

[1] Markus Jakobsson and Steven Myers. Phishing and countermeasures: understanding the increasing problem of electronic identity theft. John Wiley & Sons, Inc., 2007.

[2] Anti Phishing Working Group. Origins of the word "phishing". Available at: http://www.antiphishing.org/word_phish.htm accessed on 24/11/2016.

[3] Phishing - word spy. Available at: http://www.wordspy.com/words/phishing.asp, accessed on 27/11/2016.

[4] Available at: http://www.pcworld.com/article/135293/article.html, Accessed on 13/12/2016.

[5] Available at: http://www.phishing.org/phishing-techniques, Accessed on 13/12/2016.

[6] Available at: http://www.innovateus.net/science/what-are-different-types-phishing-attacks, Accessed on 15/12/2016.

[7] Available at: https://www.owasp.org/index.php/Session_hijacking_attack, Accessed on 16/12/2016.

[8] Available at: https://usa.kaspersky.com/internet-security-center/threats/trojans#.WF5Xhn1S6Aw, Accessed on 17/12/2016.

[9] Available at: http://en.videotutorial.ro/otravirea-dns-ului-metoda-folosita-frecvent-de-hackeri, Accessed on 17/12/2016.

[10] Available at: http://www.pcworld.com/article/135293/article.html, Accessed on 17/12/2016.

[11] Available at : https://cybercrime.org.za/data-theft, Accessed on 19/12/2016.

[12] Available at: http://www.innovateus.net/science/what-are-different-types-phishing-attacks, Accessed on 21/12/2016.

[13] Available at: http://www.computerhope.com/jargon/m/mitma.htm, accessed on: 23/12/2016.

[14] Available at: http://whatis.techtarget.com/definition/search-poisoning, Accessed on: 20/12/2016.

[15] Abdullah M.Alnajim, High Level Anti-Phishing Countermeasure: A case Study, IEEE Computer Society, 2011.

[16] Wajeb Gharibi, Some Recommended Protection Technologies for Cyber Crime on Social Engineering Techniques – Phishing, Journal of Communication and Computer, USA, Vol.8 No.7, 2011.

[17] Mishaal Abdullah Al-Kadhi, Assessment of the status of spam in the Kingdom of Saudi Arabia, Communications and Information Technology Commission, Saudi Arabia, 2011.

[18] Bushra M. Elamin, Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future, Information and Knowledge Management, Vol.3 No12, 2013.

[19] Available at: http://www.al-fanarmedia.org/2015/12/arab-universities-are-vulnerable-to-cyber-attacks-experts-say/, Accessed on: 24/12/2016.

[20] Available at: http://thehackernews.com/2012/01/saudi-arabias-king-saud-university.html, Accessed on: 26/12/2016.