A Country Based Model Towards Phishing Detection Enhancement

Abdullah M. Alnajim

Abstract— In this research, a novel country based model to detect phishing attacks is presented. The aim is to enhance the phishing countermeasures applied on a country's Internet infrastructure. This is because of that the anti-phishing framework in Saudi Arabia is exposed to users when they fall to phishing attacks. This paper proposes enhancing anti-phishing behaviors by training them to detect phishing instead of only blocking phishing websites. A prototype proof of concept implementation is discussed and shows the model is exposed to phishing victims who are inside the country deployed it (e.g. Saudi Arabia).

Index Terms— Blacklists, Content Filters, Data Service Provider, e-Commerce Security, Network Proxy, Online Banking Security, Phishing , Saudi Arabia.

I. INTRODUCTION

Security-critical applications (e.g. online banking login page) that are accessed using the Internet are at the risk of Internet fraud. Violations of security in these applications would result in severe consequences, such as financial loss for e-commerce and online banking organizations and for individuals. CyberSource [1] has revealed that financial loss due to Internet fraud is huge; in 2007, such losses amounted to $3.6 billion. As the Internet has become a vital medium of communication, Phishing can be performed in different ways. They are as follows [2]:

1. email-to-email: this occurs when someone receives an email asking for sensitive information to be replied to the sender email or sent to another email.
2. email-to-website: this occurs when someone receives an email with embedded web address that leads to a Phishing website.
3. website-to-website: this occurs when a Phishing website is reached by clicking on an online advert or through a search engine.
4. browser-to-website: this occurs when someone misspelled a web address of a legitimate website on a browser and then goes to a Phishing website that has a similar address.

There are technical advances that mitigate the problem of Phishing. For instance, security toolbars, such as SpoofStick, TrustBar and SpoofGuard, can prevent Phishing attacks. Anti-Phishing training for end-users is indispensable to any proposed technical solution. It is suggested that while technical improvements may continue to stop the attacks, end-user training is a key component in Phishing attacks mitigation [3].

In preventing online fraud, Symantec [4] believes that users' awareness is central to helping to change their behaviours and thus reduce their mistakes with Phishing emails and websites. Anti-Phishing training will make the end-user aware and it will erect an effective barrier against Phishing attempts. Anti-Phishing awareness was shown to have a great positive effect in mitigating the risk of Phishing [5]. There are different anti-Phishing training approaches to make users aware of Phishing emails and websites and to learn how to avoid them. The most basic approach is publishing guidelines for the Internet users to follow when they go online. These guidelines are referred as tips for users. All the information used in the training approaches is based on tips for users. Alnajim and Munro [6] proposed a novel anti-Phishing approach that uses training intervention (APTIPWD). The approach helps users to make correct decisions in distinguishing Phishing and legitimate websites. It brings information to end-users and helps them immediately after they have made a mistake in order to detect Phishing websites by themselves. The new approach also keeps anti-Phishing training ongoing process. This means, in all time, once users tries to submit information to Phishing website, they will be trained (see Figure 1).

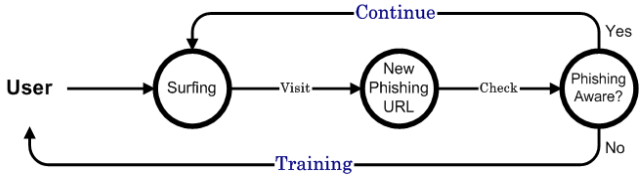

Fig. 1. The broad idea of APTIPWD

There are many anti-Phishing tips that can be used in the intervention message. The effectiveness of most common users' tips for detecting Phishing websites using novel effectiveness criteria was examined [7]. The aim of the tips' effectiveness examination was to find fewer anti-Phishing tips that users can focus on to detect Phishing attacks by themselves. Therefore, the most effective anti-Phishing tip was used [6]. The tip was as follows: "a fake website's address is different from what you are used to, perhaps there are extra characters or words in it or it uses a completely different name or no name at all, just numbers. Check the True URL (Web Address). The true URL of the site can be seen in the page 'Properties' or 'Page Info': While you are on the website and using the mouse Go Right Click then Go 'Properties' or 'Page Info'. If you don't know the real web address for the legitimate organization, you can find it by using a search engine such as Google".

Revised Version Manuscript Received on June 09, 2015.

Dr. Abdullah M. Alnajim, Department of Information Technology, College of Computer, Qassim University, Buraydah, Saudi Arabia.

In this paper, research will be conducted to propose a country based model to detect phishing attacks. This model is a result of applying the idea proposed previously in Fig 1 on the current anti-phishing framework implemented in Saudi Arabia presented in a previous research [8]. The aim is to enhance the phishing countermeasures applied on a country Internet infrastructure. In this research, there is an assumption that Phishing attacks do not use either software to change the host files in users' operating systems or any malicious software, such as a virus, worm or Trojan horse, that runs in users' operating systems. These are called 'Pharming' and 'Malware' and are different from Phishing. Phishing is a deceptive attack which aims to take advantage of the way humans interact with computers or interpret messages rather than taking advantage of the technical system vulnerabilities [9]. The remainder of the paper is organized as follows. Section two reviews the literature regarding Phishing detection methods and shows a high level (a country-based) anti-phishing countermeasure that is implemented in Saudi Arabia. The third section presents the proposed model that is applied on a country framework to detect phishing attacks. The fourth section discusses and analyses the pros and cons of the proposed model. The final section concludes the paper and discusses the possible way of future work.

II. RELATED WORK

A. Phishing Detection

There are technical (e.g. toolbars) and training (e.g. tips) approaches to mitigate Phishing. The anti-Phishing toolbars are web browser plug-ins that warn users when they reach a suspected Phishing site [9]. Anti-Phishing tools use two major methods for mitigating Phishing sites. The first method is to use heuristics to check the host name and the URL for common spoofing techniques. The second method is to use a blacklist that lists Phishing URLs. The heuristics approach is not 100% accurate since it produces low false negatives (FN), i.e. a Phishing site is mistakenly judged as legitimate, which implies they do not catch all Phishing sites. The heuristics often produce high false positives (FP), i.e. incorrectly identifying a legitimate site as fraudulent. Blacklists have a high level of accuracy because they are constructed by paid experts who verify a reported URL and add it to the blacklists if it is considered as a Phishing website [10]. Many financial and commercial, private and government institutions (e.g. eBay and HSBC) have provided anti-Phishing training tips for detecting Phishing emails and websites. The aim of the tips is to train users to look for Phishing clues located in emails and websites to enable them to make better decisions in distinguishing Phishing emails and websites. People in general do not read anti-Phishing online training materials although some of them are found effective when used [7]. Many commercial institutions, such as Microsoft, periodically send email security information to help their customers in protecting their online security [11]. This email provides practical security tips, useful resources and links, and a forum to ask security-related questions. Microsoft states that the email is suitable for customers to stay up to date on the latest issues and events with:

- Security tips including anti-Phishing tips.
- Security critical updates.
- Answers to frequently asked questions (FAQs) on security topics.
- Information about security trials and downloads.
- Tips from security team for home users.

Theses emails are usually sent in text and HTML formats. The limitation of this approach is that customers who are interested in receiving these emails need to subscribe with the commercial institutions (i.e. anti-Phishing emails providers) in order to be included in receiving these emails. An online game was proposed in order to teach users good habits to help them avoid Phishing attacks [12]. Kumaraguru et al [13] considered training people about Phishing email during their normal use of email. Their aim was to teach people what Phishing clues to look for located in emails. They found that email training approach works better than the current practice of publishing or sending anti-Phishing tips.

B. High Level Phishing Detection in Saudi Arabia

The Internet was first established in Saudi Arabia officially in 1997 by a ministerial decision whereas the Internet was first made available to the public in 1999 [14]. In December 2000, the number of Internet users was just 200,000 and this number has grown sharply to 18,300,00 users by June 2010 out of 27 millions of residents in the country [15].The structure of the Saudi Arabian Internet enforces all URLs' requests made by local Internet users to go through a content filtering system. The filtering takes place in order to block web pages that contain pornographic, harmful, offensive and objectionable issues to the user in particular and to the community in general [16]. The filtering method was established and supervised by the Internet Services Unit (ISU) at the King Abdulaziz City of Science and Technology (KACST). However, since 2006, the supervision of the filtering system has been transferred to the Communications and Information Technology Commission (CITC) and deployed by three new Data Service Providers (DSPs)1. The CITC now supervises the Internet in the country and maintains blacklists that contain all blocked websites. The blacklists are daily updated by information security experts and given to DSPs. DSPs in turn distribute the Internet services to Internet Services Providers ISPs2. When one of the DSPs proxies receives a URL request from ISPs users, the URL compared to the blacklists. If the URL is blacklisted, the user is redirected to a blocking page (see Figure 2) developed by CITC.

1 Data Service Provider (DSP) means companies or organizations that provide the major gateways to the International Internet. Since summer 2006 there have been three licensed commercial Data Service Providers in Saudi Arabia [17]. They are Saudi Telecommunications Company, Integrated Telecommunications Co Ltd and Bayanat Al Oula for Network Services [18].

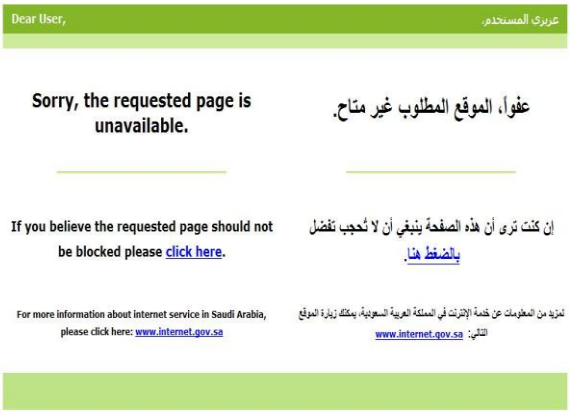

Fig. 2. The CITC's blocking page

In a previous research [8], an introduction and analysis were carried out for a high level (a country-based) anti-phishing countermeasure implemented in Saudi Arabia. The research examined how this countermeasure is effective against phishing scenarios. The research described the scenario occurs when a Phishing attack is reported. This scenario is described in detail in a model illustrated on Figure 3. As shown on Figure 3, once a bank or a commercial institute realizes that there is a phishing attack targeting their customers, they notify two bodies. They are

1. The organization that hosts the phishing website to request URL shutdown. This step followed if the website is hosted by an international hosting organization. Otherwise this step omitted and the notification should be passed only to the following second body.
2. The Saudi Arabian Monetary Agency (SAMA) which supervises all the financial institutions (e.g. banks) in the country to start internal anti-phishing procedures.

The SAMA in turns passes the 'phishing URL notification' to the CITC. Once the notification arrives to the CITC information security team, it is checked and assured by experts. Having done 'phishing URL assurance', the URL is added to the blacklist. Then the CITC provides the DSPs with the new blacklists update. It takes 30-60 minutes for a URL to be checked and blacklisted. After updating the blacklist, when a local Internet user in Saudi Arabia requests a reported phishing URL, they are redirected to the blocking page illustrated on Figure 2. Later on, the international or national hosting organizations is contacted by SAMA and they should investigate and shutdown any reported URL which takes 3-6 days in average and maximum of one month according to the APWG3. The location of the source or the destination of Phishing attacks is vital in the analysis of the model because the model works only in Saudi Arabia. Hence, based on the location, the scenarios used in the analysis should come across all possible sources of Phishing attacks as well as all possible destinations of Phishing attacks.

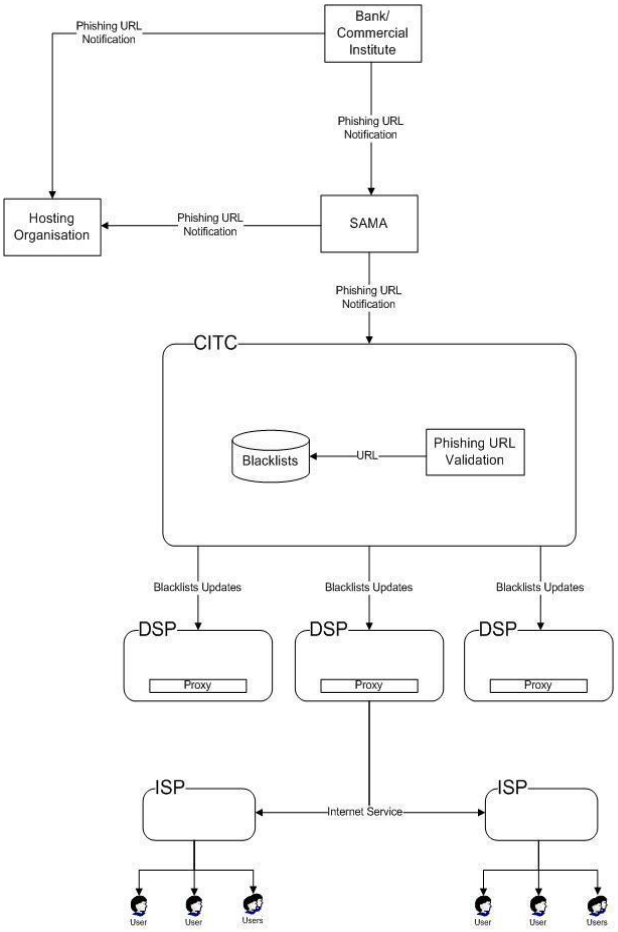

Fig. 3. The Anti-Phishing Detection Framework in Saudi Arabia.

Because of this, the effectiveness of the model shown on Figure 3 was examined against all possible Phishing attacks scenarios initiated by or designed to attack users inside and outside Saudi Arabia.

assumption(I): the blacklists used by the model are up-to-date and effective. This means any reported Phishing URL is verified and added swiftly by experts.

assumption(II): the hosting national or international organizations have the full responsibility for shutting down any Phishing URL. They may response to any official request from SAMA or any bank/commercial institute swiftly and they may not response at all. Therefore, the model has no control over shutting down websites by their hosting organizations. Because of this, this research assumes the worst case that may happen which is that hosting organizations do not shut down Phishing websites for any reason.

Table1: Model Effectiveness Against All Possible Phishing Scenarios

Source / Destination	Internal	External
Internal	effective	effective
External	ineffective	ineffective

[2] Internet Service Provider (ISP) buys Internet bandwidth from the DSPs and provides Internet connections to the companies and individuals [19].
3 Anti-Phishing Working Group, www.apwg.com.

Table 1 shows the effectiveness of the model against all possible Phishing scenarios. These scenarios are model-location based. This means that the central location of the model is Saudi Arabia so that internal and external implies inside and outside Saudi Arabia respectively. There are four scenarios may occur. They are as follows (See Table 1):

1. Internal Source – Internal Destination: this scenario happens when (a) an attacker launches a Phishing website hosted by an organization located inside Saudi Arabia and (b) a user inside Saudi Arabia surfs a Phishing website. With regard to this scenario, the model is effective because the local (i.e. located in Saudi Arabia) Internet user cannot reach the Phishing website. Therefore, the model prevents the user from falling in Phishing.
2. Internal Source – External Destination: this scenario happens when (a) an attacker launches a Phishing website hosted by an organization located inside Saudi Arabia and (b) a user outside Saudi Arabia surfs a Phishing website. With regard to this scenario, the model is ineffective because the user may reach the Phishing website. Therefore, the model does not prevent the user from falling in Phishing.
3. External Source – Internal Destination: this scenario happens when (a) an attacker launches a Phishing website hosted by an organization located outside Saudi Arabia and (b) a user inside Saudi Arabia surfs a Phishing website. With regard to this scenario, the model is effective because the local (i.e. located in Saudi Arabia) Internet user cannot reach the Phishing website. Therefore, the model prevents the user from falling in Phishing.
4. External Source – External Destination: this scenario happens when (a) an attacker launches a Phishing website hosted by an organization located outside Saudi Arabia and (b) a user outside Saudi Arabia surfs a Phishing website. With regard to this scenario, the model is ineffective because the user may reach the Phishing website. Therefore, the model does not prevent the user from falling in Phishing.

   Having discussed the scenarios, it is obvious that the model is effective when the websites are reached by users who surf the Internet from inside Saudi Arabia whereas it is ineffective in protecting users from falling in phishing when the websites are reached by users who surf the Internet from outside Saudi Arabia.

III. THE NEW MODEL

A. Objective

Due to that the anti-phishing framework in Saudi Arabia presented in Figure 3 is exposed to users when they fall to phishing attacks. Thus enhancing anti-phishing behaviors by training them to detect phishing instead of only blocking phishing websites is proposed. The idea presented by Alnajim and Munro [6] is applied on the current anti-phishing framework implemented in Saudi Arabia. Making use of this framework to enhance the anti-phishing behaviors for users is proposed. Therefore, a novel country based model to detect phishing attacks is presented in this section. The aim is to enhance the phishing countermeasures applied on a country's Internet infrastructure.

B. Model and Scenarios

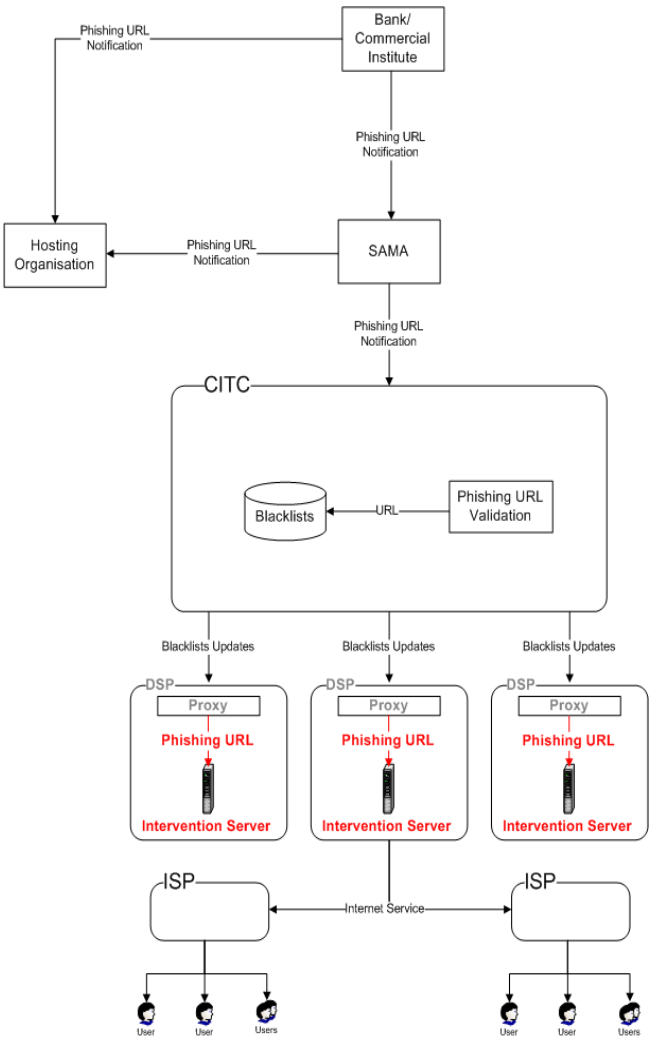

Fig. 4: The proposed Intervention Server (in red color)

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

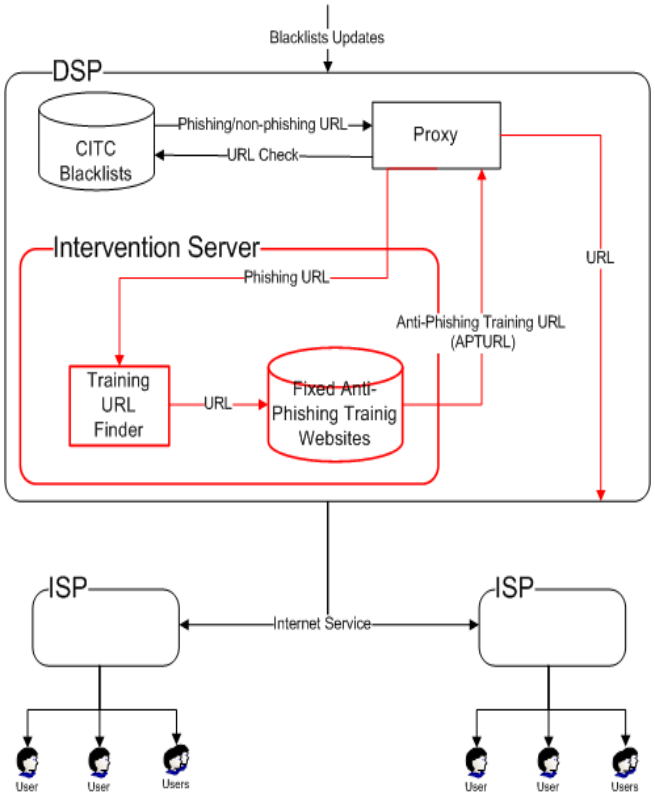

Fig. 5: Components of the Proposed Intervention Server (in red color)

The black lists updates come from the Communications and Information Technology Commission (CITC) as an input to Data Service Providers (DSPs)4. Figure 4 shows that each DSP has got its own proxy. Therefore, if a user requests a URL, the DSP proxy directs the URL to CITC blacklists to check whether the URL is blacklisted or not (see Figure 5). The CITC blacklists replies the results. If the URL is non-phishing, then Proxy responds to it based on the DSP instructions. This case is not the research focus. However, if the URL is a phishing then the Proxy redirects the URL to the Intervention Server (IS). Once the IS receives a notification that a phishing URL is requested, an agent named 'Training URL Finder' (TURLF) connects to a database that include a Fixed Anti-Phishing Training Websites. The IS runs these websites locally. TURLF is responsible for recognizing the suitable Anti-Phishing Training URL (APTURL) for the Phishing URL redirected from the Proxy. Thus, the TURLF is assumed that it returns to the Proxy the APTURL dedicated for the website that is being attacked by the phishing URL. Finally, the Proxy sends to the user the dedicated APTURL as a response to the user request initiated in the beginning.

IV. SIMULATION AND DISCUSSION

A prototype proof of concept implementation is presented in this section. In order to test the approach's effectiveness, simulating the possible scenarios is needed. The websites used in the experiments were identical copies of the real ones. The legitimate and Phishing websites were stored on the local machine and run by Apache server. All the Phishing emails and websites used for this experiment were based on real ones collected from various Phishing examples resources. The DNS (Domain Name System) host files in Windows operating system was modified so that web browsers displayed the URL of the actual Phishing websites. All Phishing websites were functional so their users were able to submit information. Having implemented the model as a prototype proof of concept, the new model shown in figures 4 and 5 is exposed to phishing victims who are inside the country deployed it (e.g. Saudi Arabia). This enhances the anti-phishing countermeasures deployed nowadays in Saudi Arabia shown in figure 3. In the other hand, the limitation could be that it makes the Internet traffic a little bit slower. This is because of extra component (i.e. Intervention Server) added to the anti-phishing detection framework in Saudi Arabia shown in figure 3.

4 Data Service Provider (DSP) means companies or organizations that provide the major gateways to the International Internet. Since summer 2006 there have been three licensed commercial Data Service Providers in Saudi Arabia [17]. They are Saudi Telecommunications Company, Integrated Telecommunications Co Ltd and Bayanat Al Oula for Network Services [18].

V. CONCLUSION

In this research, a novel country based model to detect phishing attacks is presented. The aim is to enhance the phishing countermeasures applied on a country's Internet infrastructure. This is because of that the anti-phishing framework in Saudi Arabia presented in Figure 3 is exposed to users when they fall to phishing attacks and thus enhancing anti-phishing behaviors by training them to detect phishing instead of only blocking phishing websites is proposed. The idea presented by Alnajim and Munro [6] is applied on the current anti-phishing framework implemented in Saudi Arabia. Having implemented the model as a prototype proof of concept, The new model has advantages and limitations. The advantage is that the model is exposed to phishing victims who are inside the country deployed it (e.g. Saudi Arabia). This enhances the anti-phishing countermeasures deployed nowadays in Saudi Arabia shown in figure 3. Whereas a potential drawback could be that it makes the Internet traffic a little bit slower. This is because of extra component (i.e. Intervention Server) added to the anti-phishing detection framework in Saudi Arabia shown in figure 3.

REFERENCES

1. CyberSource. (2008). *9th Annual Online Fraud Report*. Available: http://www.cybersource.com, last access on 20/3/2007.
2. A. Alnajim, and M. Munro, 2009. "An Approach to the Implementation of the Anti-Phishing Tool for Phishing Websites Detection". Proc. International Conference on Intelligent Networking and Collaborative Systems (INCoS 2009). Barcelona, Spain: IEEE Press, pp. 105 - 112.
3. S. A. Robila and J. W. Ragucci, "Don't be a Phish: Steps in User Education". Proc. 11th annual SIGCSE conference on innovation and technology in computer science education. New York: ACM Press, 2006, pp. 237 – 241.
4. Symantec. (2004). *Mitigating Online Fraud: Customer Confidence, Brand Protection, and Loss Minimization*. Available: http://www.antiphishing.org/sponsors_technical_papers/symantec_online_fraud.pdf, last access on 21/3/2007.
5. A. Alnajim and M. Munro, "Effects of Technical Abilities and Phishing Knowledge on Phishing Websites Detection". Proc. the IASTED International Conference on Software Engineering (SE 2009), Innsbruck, Austria, ACTA Press, 2009, pp. 120-125.

6. A. Alnajim and M. Munro, "An Anti-Phishing Approach that Uses Training Intervention for Phishing Websites Detection". Proc. 6th IEEE International Conference on Information Technology - New Generations (ITNG). Las Vegas, IEEE Computer Society, 2009, pp. 405-410.
7. A. Alnajim and M. Munro, "An Evaluation of Users' Tips Effectiveness for Phishing Websites Detection". Proc. 3rd IEEE International Conference on Digital Information Management ICDIM, London, IEEE Press, 2008, pp. 63-68.
8. A. Alnajim, "High Level Anti-Phishing Countermeasure: A Case Study". Proc. The The World Congress on Internet Security (WorldCIS-2011), London, UK, IEEE Press, 2011, pp. 139 – 144.
9. J. S. Downs, M. B. Holbrook and L. F. Cranor, "Decision strategies and susceptibility to phishing". Proc. the 2nd symposium on usable privacy and security. New York, USA: ACM Press, 2006, pp. 79 – 90.
10. Y. Zhang, J. I. Hong and L. F. Cranor, "Cantina: a content-based approach to detecting phishing web sites". Proc. 16th international conference on WWW. New York: ACM Press, 2007, pp. 639 – 648.
11. Microsoft Corporation. (2007). *Microsoft Security for Home Computer Users Newsletter*. Available: http://www.microsoft.com/protect/secnews/default.mspx, last access on 16 March 2007.
12. S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong and E. Nunge, "Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish". Proc. 3rd symposium on usable privacy and security SOUPS. New York: ACM Press, 2007, pp. 88 – 99.
13. P. Kumaraguru, Y. Rhee, A. Acquisti, L. F. Cranor, J. Hong and E. Nunge,"Protecting people from phishing: the design and evaluation of an embedded training email system". Proc. the SIGCHI conference on Human factors in computing systems. New York, USA: ACM Press, 2007, 905 – 914.
14. Communications and Information Technology Commission CITC. (2010). *Internet in Saudi Arabia*. Available: http://www.internet.gov.sa/learn-the-web/guides/internet-in-saudi-arabia/view?set_language=en, last access on 22 November 2010.
15. Miniwatts Marketing Group. (2015). *Internet World Stats*. Available: http://www.internetworldstats.com/middle.htm, last access on 14 March 2015.
16. Communications and Information Technology Commission CITC. (2007). *Content filtering in Saudi Arabia*. Available: http://www.internet.gov.sa/learn-the-web/guides/content-filtering-in-saudi-arabia, last access on 20 June 2007.
17. Communications and Information Technology Commission CITC. (2007). *Data Service Provider*. Available: http://www.internet.gov.sa/learn-the-web/glossary/data-service-provider-dsp/view?set_language=en, last access on 20 June 2007.
18. Communications and Information Technology Commission CITC. (2007). *List of Service Providers*. Available: http://www.internet.gov.sa/learn-the-web/guides/list-of-service-providers/view?set_language=en, last access on 20 June 2007.
19. Communications and Information Technology Commission CITC. (2007). *Internet Service Provider*. Available: http://www.internet.gov.sa/learn-the-web/glossary/internet-service-provider, last access on 20 June 2007.

Author Profile

Dr. Abdullah M. Alnajim is an information security and academic consultant. He is also a faculty in the Information Technology Department, college of Computer at Qassim University, Saudi Arabia. Dr. Abdullah Alnajim had BSc in Computer Science from King Saud University in Saudi Arabia in 2002. Dr. Alnajim had MSc in Internet and Distributed Systems from Durham University in the United Kingdom in 2005. Dr. Alnajim had a Ph.D from the Department of Computer Science at Durham University in 2009. His Ph.D thesis was entitled as 'Fighting Internet Fraud: Anti-Phishing Effectiveness for Phishing Websites Detection'. Dr. Alnajim's research interests involve Internet security and frauds that encounter web applications especially online banking and e-commerce applications.