An Approach to the Implementation of the Anti-Phishing Tool for Phishing Websites Detection

Abdullah Alnajim
Department of Computer Science
Qassim University
Buraydah, Saudi Arabia
abdullah.alnajim@yahoo.com

Malcolm Munro
Department of Computer Science
Durham University
Durham, United Kingdom
malcolm.munro@durham.ac.uk

Abstract— **Phishing attacks have become a serious problem for users of online banking and e-commerce websites. A previous study proposed and evaluated a novel anti-Phishing approach that uses training intervention for Phishing websites detection (APTIPWD). The proposed approach showed that it helped users to make correct decisions in distinguishing Phishing and legitimate websites. In this paper, an approach to the implementation of the APTIPWD is presented. It also shows that the APTIPWD is feasible and can be implemented within any proxy-based network easily without writing a single line of a programming code and without undue disruption of the users system.**

Keywords— Phishing, network proxy, blacklists, anti-Phishing countermeasures, e-commerce security, online banking security.

I. INTRODUCTION

THE Internet is a very important medium of communication. Many people go online and conduct a wide range of business. They can send emails, sell and buy goods, transact various banking activities and even participate in political and social elections by casting a vote online. Once users go online, they are at risk from online fraud (also known as Internet fraud). Internet fraud is a crime that uses the Internet as the medium to carry out financial frauds [1]. The parties involved in any transaction never need to meet and the user may have no idea whether the goods or services exist. Due to this, the Internet is a good vehicle to defraud people who use it to buy goods or services [1]. The application access keys could be stolen. Applications such as electronic commerce, electronic banking, electronic voting and electronic mail are targets for fraudsters.

Security for conducting businesses online is vital and critical. All 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 [2] has revealed that financial loss due to Internet fraud is huge; in 2007, such losses amounted to $3.6 billion.

Internet fraud has a multiplicity of forms, including Phishing attacks. Phishing is an attack that seeks to trick people into revealing sensitive information about themselves and their internet accounts [3]. Phishing aims to take advantage of the way humans interact with computers rather than taking advantage of technical system vulnerabilities [3]. Phishing is about other parties attempting to gain personal information such as bank details and passwords. As the Internet has become a vital medium of communication, Phishing can be performed in different ways. They are as follows:

1. email-to-email: this happens 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 happens when someone receives an email with embedded web address that leads to a Phishing website.
3. website-to-website: this happens when a Phishing website is reached by clicking on an online advert or through a search engine.
4. browser-to-website: this happens 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.

Phishing scams have become a problem for online banking and e-commerce users [4]. Gartner conducted a survey of 3,985 individuals in September 2008 to determine consumer Phishing trends [5]. The percentage of Phishing victims is higher than ever. 5 million Internet users in the United States were victims in 2008. This is an increase of 40 percent over 2007 [5]. According to the survey, 4.3 percent of people who received Phishing emails lost money from the attack (compared to 3 percent in 2005). Litan believed that '*a four percent successful response rate is quite good, considering legitimate mass email marketing campaigns have a success rate of about 1.5 percent*'.

978-0-7695-3858-7/09 $26.00 © 2009 IEEE
DOI 10.1109/INCOS.2009.37

Some technical advances 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 [6]. In preventing online fraud, Symantec [7] 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 [8].

There is a variety of 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. We refer to these guidelines as tips for users. All the information used in the training approaches is based on tips for users.

Alnajim and Munro [9] 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).

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 [10]. The effectiveness criteria consisted of four criterions. The effectiveness criteria were as follows:

1. The tip prevents the most common clue.
2. Solo reliability. This criterion means that the evaluated tip is enough to detect and prevent Phishing attack.
3. The clue cannot be spoofed. In other words, the evaluated tip cannot be changed or faked by fraudster.
4. The tip does not produce false positives FP or false negatives FN. This means that by using the tips, the decision made will not be FN or FP. 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 [9]. 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*".

The APTIPWD was evaluated using users experiments [9]. There were three groups; Control, Old Approach and New Approach. There were 36 participants in the experiment. Each group had 12 participants. They found that there is a significant positive effect of using their approach in comparison with an old approach of sending anti-Phishing tips by email. Their approach is better in helping users properly judge legitimate and Phishing websites.

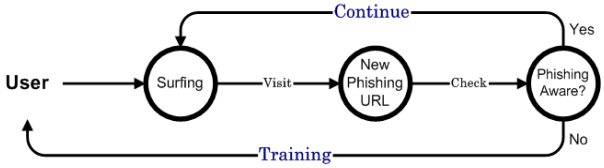

Fig 1. The broad idea of APTIPWD

In this paper, an approach to the implementation of the APTIPWD is presented. It also shows that the APTIPWD is feasible and can be implemented within any proxy-based network easily without writing a single line of a programming code and without undue disruption of the users system.

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 [3].

The remainder of the paper is organized as follows. Section two looks at the literature regarding Phishing countermeasures and an overview of the concept of proxy based computer network. The third section describes the approach to the implementation of the APTIPWD and applying it to a proxy based computer network. The fourth section presents discussions on the advantages and the possible limitation of the APTIPWD and the final section concludes the paper and discusses the possible way of future work.

II. Related Work

A. Anti-Phishing Countermeasures

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 [3]. 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 [11].

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 [10].

Many commercial institutions, such as Microsoft, periodically send email security information to help their customers in protecting their online security [12]. 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 [13]. Kumaraguru et al [14] 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. However, Kumaraguru et al's approach does not consider teaching people with Phishing website-related tips. Phishing sites can be reached via various methods in addition to emails such as online advertisements.

B. Proxy based Computer Network

1) *General*

A client-server model is a common design for distributed computing. The client and the server are two components that interact between each other [15].

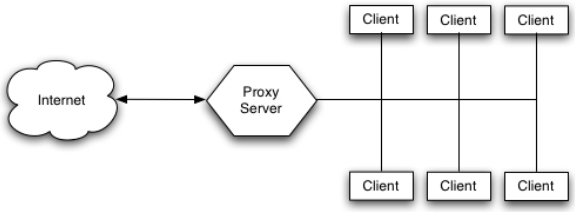

Fig 2. Server-Proxy-Client Interaction[1]

A client-proxy-server model extends the client-server model [16]. It introduces an additional component which is a proxy. The proxy is located between the client and the server [16]. Figure 2 presents an overview of the interaction between the client, proxy and server. The server component is represented by the "Internet" because in a proxy based computer network, any URL request to the web made by a client is directed to the URL domain server. Proxies have been widely used in many applications to perform various tasks such as

- clients' connections control,
- URLs' request control,
- caching and
- filtering data [17].

2) *How it Works*

The interaction between client and server is as follows [15]:

- Client requests a service from Server.
- Server processes the requests and replies to Client.

However, in the client-proxy-server, the interaction becomes as follows:

- Client sends request for Server to Proxy.
- Proxy passes request to Server.
- Server processes the request and sends reply for the Client to Proxy.
- Proxy passes reply to Client.

III. APPLYING THE (APTIPWD) TO A PROXY BASED COMPUTER NETWORK

In this section, the APTIPWD is applied to a proxy based network. The design and implementation are described.

A. System Design with Fixed List of Phishing Websites

As shown in Figure 3, the design of the APTIPWD system consists of four components. They are:

- Server,
- Proxy (Gateway),
- Administrator, and

[1] Source: ServerWatch.com, available at: http://www.serverwatch.com/tutorials/article.php/10825_3092521_1, last access on 15 November 2008

- Client (User).

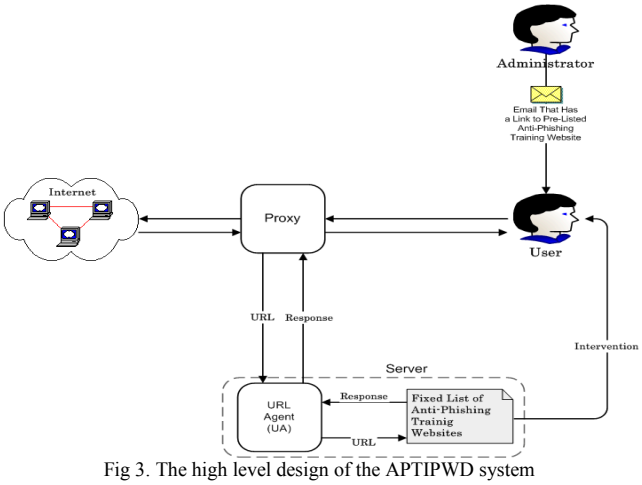

Fig 3. The high level design of the APTIPWD system

The Administrator is a person who is in charge of sending Phishing emails to any User in a network. The Proxy is in place between the Internet and Users. The Proxy acts as a gateway for all requests made in the network by its Users. Any URL request made by a User goes through the Proxy. The Proxy then communicates with the Server. The Server contains three sub-components. They are a Fixed List of Anti-Phishing Training Websites (FLAPTW), a URL Agent (UA) and the Intervention message. The FLAPTW contains a fixed number of fake websites that are designed to look the same as the original ones and to be used for anti-Phishing training only, whereas the UA is responsible for checking whether the requested URL passed by the Proxy is in the FLAPTW. The Intervention message is stored in the Server. It is shown to the User in order to help them understand what Phishing is and how to detect it in the future.

1) Scenario

The Administrator sends the anti-Phishing training email to specific Users. The email contains a link (URL) for one of the FLAPTW. If the User goes to the URL, browses the URL page and clicks to submit information, the UA verifies whether or not the URL is listed in the FLAPTW by checking the FLAPTW. If the URL is listed, the UA retrieves the intervention message and presents it to the User. Otherwise, the Proxy allows the User to browse the Internet as normal.

2) Assumption

There is an assumption that the Administrator is given the privilege in the network email system to send anti-Phishing training email that bypasses the anti-Phishing filters that might be applied in the network email system. This means that the anti-Phishing training email should have the following characteristics:

- The domain of the sender's email should be the same as the domain of a legitimate website.
- The email content should look as it is legitimate email.

B. Implementation

In this section, the implementation of the components of the APTIPWD is presented. Each component's implementation is described separately.

1) Server

The Server component was implemented using Apache HTTP Server. Apache HTTP Server is an open-source web Server for popular operating systems such as UNIX and Windows [18]. A 1.40GHz Toshiba laptop, which runs Microsoft Windows XP home edition, was used to run the Apache HTTP Server.

The Server's sub-components, the URL Agent (UA), the Fixed List of Anti-Phishing Training Websites (FLAPTW) and the Intervention message, were linked to each other. The UA received any URL from the Proxy and directed it to either the local server (i.e. the prototype's Server) or the requested website on the Internet. This was accomplished by the virtual hosts[2] directives in Apache HTTP Server. The virtual hosts' container is a configuration file that contains all the web addresses that were served locally by the Server when requested (see Figure 4). However, this container had to be pointed by the main Apache HTTP Server's configuration file (see Figure 5).

```
#
# VirtualHost example:
# Almost any Apache directive may go into a VirtualHost container.
# The first VirtualHost section is used for all requests that do not
# match a ServerName or ServerAlias in any <VirtualHost> block.
#
<VirtualHost *:80>
    DocumentRoot "C:/Program Files/Apache Software Foundation/Apache2.2/htdocs"
    ServerName localhost
    ErrorLog "logs/localhost-error.log"
    CustomLog "logs/localhost-access.log" common
</VirtualHost>

<VirtualHost *:80>
    DocumentRoot C:/mysites/amazonme
    ServerName www.amazon.co.uk.me.com
    ErrorLog "logs/www.amazon.co.uk.me.com-error.log"
    CustomLog "logs/www.amazon.co.uk.me.com-access.log" common
</VirtualHost>

<VirtualHost *:80>
    DocumentRoot C:/mysites/citybank
    ServerName www.citybank.co.uk
    ErrorLog "logs/www.citybank.co.uk-error.log"
    CustomLog "logs/www.citybank.co.uk-access.log" common
</VirtualHost>

<VirtualHost *:80>
    DocumentRoot C:/mysites/halifaxme
    ServerName www.halifax-online.co.uk.me.com
    ErrorLog "logs/www.halifax-online.co.uk.me.com-error.log"
    CustomLog "logs/www.halifax-online.co.uk.me.com-access.log" common
</VirtualHost>

<VirtualHost *:80>
    DocumentRoot C:/mysites/argosmyshop
    ServerName www.argos.co.uk.myshop.com
    ErrorLog "logs/www.argos.co.uk.myshop.com-error.log"
    CustomLog "logs/www.argos.co.uk.myshop.com-access.log" common
</VirtualHost>

<VirtualHost *:80>
    DocumentRoot C:/mysites/cometonline
    ServerName www.comet-online.co.uk
    ErrorLog "logs/www.comet-online.co.uk-error.log"
    CustomLog "logs/www.comet-online.co.uk-access.log" common
</VirtualHost>
```
Fig 4. Examples of virtual hosts' directives in their container

```
# Virtual hosts
Include conf/extra/httpd-vhosts.conf
```
Fig 5. Pointing virtual hosts' container in Apache configuration file

In addition, the DNS[3] host files in the Windows operating system were modified so that web browsers displayed the

[2] Virtual Host is defined as the practice of running more than one website, such as www.example1.com and www.example2.com, on a single machine [19].

[3] DNS stands for Domain Name System. The DNS main task is mapping symbolic host names to their IP addresses [20].

URL of the actual Phishing websites. As Figure 6 illustrates, the web addresses listed were pointed to the local machine IP address (127.0.0.1) so that any request to one of the addresses that arrived at the Apache HTTP Server was directed to and served by the local server. Thus, the users were not actually at risk since they used local web pages.

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost

127.0.0.1       www.ebay-security.com
127.0.0.1       www.paypa1.com
127.0.0.1       www.online.ll0ydstsb.co.uk
127.0.0.1       www.amazon.co.uk.me.com
127.0.0.1       www.barclaysbanking.co.uk
127.0.0.1       www.halifax-online.co.uk.me.com
127.0.0.1       www.citybank.co.uk
127.0.0.1       www.capital0ne0nline.co.uk
127.0.0.1       www.co-operattivebank.co.uk
127.0.0.1       www.comet-online.co.uk
127.0.0.1       www.argos.co.uk.myshop.com
```

Fig 6. Screenshot of the modified DNS host file used for the prototype

As seen in Figure 4, the every single virtual host pointed a single location for a website pages directory stored in the Server. Thus, there was a directory for each anti-Phishing training website. As shown in Table 1, eleven websites were used. They were a fixed list of anti-Phishing training websites (FLAPTW). There were different URL syntax's tricks (i.e. Phishing clues). They formed the URLs for the Phishing websites. They were as follows:

- URLs with a different domain from a well-known domain (DD),
- URLs with misspelled known websites (Miss) and
- URLs with large host names that contained a part of a well-known web addresses (LHN).

TABLE 1
THE FIXED LIST OF ANTI-PHISHING TRAINING WEBSITES USED IN THE PROTOTYPE

#	Anti-Phishing Training Websites	URL	Tricks
1	eBay	www.ebay-security.com	DD
2	Paypal	www.paypa1.com	Miss
3	Lloyds TSB Bank	www.online.ll0ydstsb.co.uk	Miss
4	Amazon	www.amazon.co.uk.me.com	LHN
5	Barclays Bank	www.barclaysbanking.co.uk	DD
6	Halifax Bank	www.halifax-online.co.uk.me.com	LHN
7	Citibank	www.citybank.co.uk	Miss
8	Capital One	www.capital0ne0nline.co.uk	Miss
9	Cooperative Bank	www.co-operattivebank.co.uk	Miss
10	Comet	www.comet-online.co.uk	DD
11	Argos	www.argos.co.uk.myshop.com	LHN

Each one of the websites was linked to the intervention message by modifying the submission button so that it transferred the traffic to the intervention message. The intervention message was a simple HTML page adjusted by JAVA scripts to appear as a pop up window and to locate in the middle of the screen. Figure 7 presents the intervention message used in the prototype. The LHN, Miss and DD tricks shown in Table 1 can be overcome by reading and understanding the intervention message.

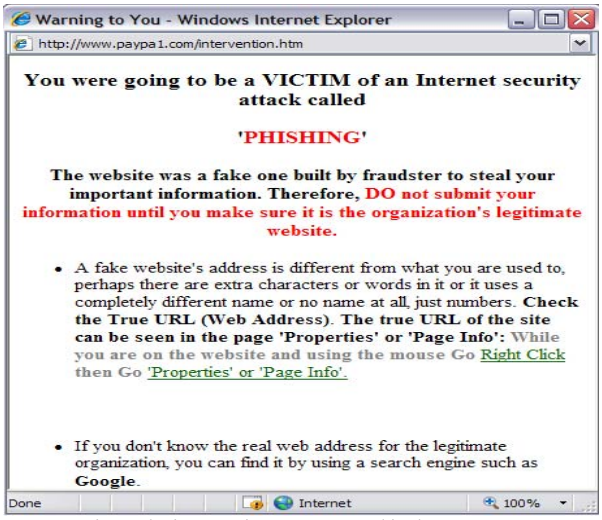

Fig 7. The intervention message used in the prototype

2) *Proxy (Gateway)*

The Proxy component was implemented using Apache HTTP Server because it has proxying capabilities that are useful and very easy to implement. The Proxy was implemented by activating the proxy module in the Server. As shown in Figure 8, the Apache HTTP Server configuration file was modified so that the proxy was able to do caching and to handle http and secure http requests. Therefore, the Proxy deals with all requests made to a specific port, which is 80.

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule cache_module modules/mod_cache.so
LoadModule disk_cache_module modules/mod_disk_cache.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so

<IfModule mod_proxy.c>
ProxyRequests On
AllowCONNECT 80 443
<Proxy *>
Order deny,allow
Deny from all
Allow from 192.168.1.65
</Proxy>
</IfModule>
```

Fig 8. The proxy module in the Server's configuration file

3) *Administrator*

There was no Graphical User Interface (GUI) implemented for the Administrator part. Microsoft Outlook was used instead. Microsoft Outlook has Email Accounts settings where people can provide sender name and email address. Therefore, the Administrator provided false sender name and email address that appeared as it was issued by a legitimate organization such as eBay (see Figure 9).

Due to that the fake emails were read using Maktoob email portal [21], the fake emails were sent by using Maktoob's MX Record[4] as the outgoing mail or server. The outgoing mail settings were adjusted in Microsoft Outlook (see Figure 9).

After setting the Email Account information, the Administrator could send an email with content that looked authentic and similar to that used by a legitimate organization. As shown in Figure 10, the emails sent by the Administrator had links to anti-Phishing training websites stored and run by the Apache HTTP Server discussed previously.

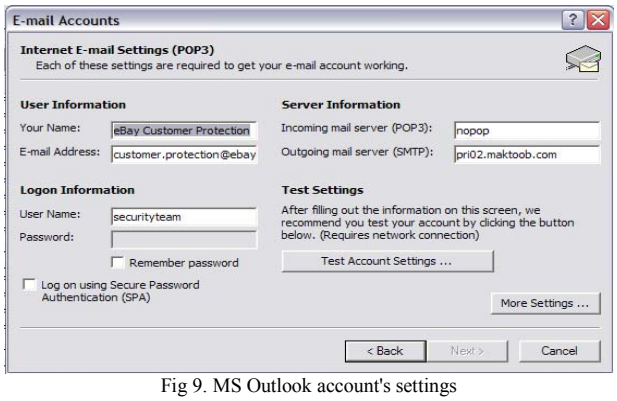

Fig 9. MS Outlook account's settings

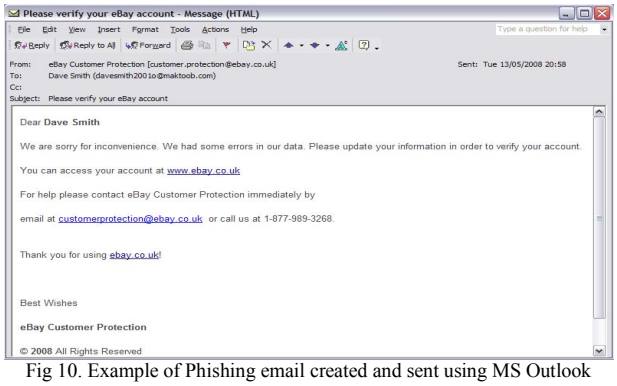

Fig 10. Example of Phishing email created and sent using MS Outlook

4) *Client (User)*

There was no implementation required for the client side of the prototype. The user used the Internet Explorer (IE) 7 browser for accessing emails and websites through Maktoob mail portal [21]. Figure 11 shows a screenshot of the eBay anti-Phishing training website used in the APTIPWD System.

[4] It stands for *mail exchange record*. It is an entry in a domain name database that identifies the mail server that is responsible for handling emails for that domain name. More information can be found at http://www.goecart.com/domain-name-terms-glossary.asp, last access on 19 September 2008.

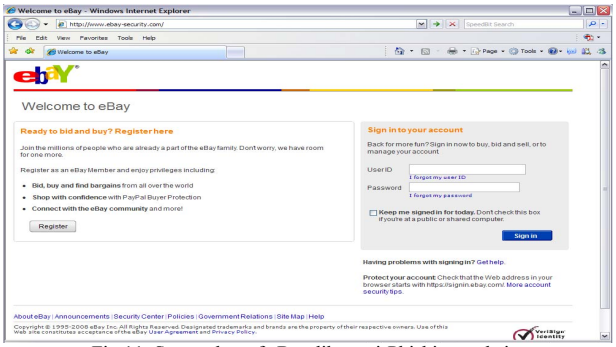

Fig 11. Screenshot of eBay-like anti-Phishing website

C. *Configuring Clients' Local Area Network (LAN) Settings to Speak to the Proxy*

In a proxy based computer network, the proxy settings in the LAN settings of every single machine (client) that is connected to it should be configured so that the address of the proxy is provided with its port. For example, clients in Durham University network applied the university proxy in their LAN settings[5]. Therefore, each client was connected to the Proxy to request any URL. This was carried out by putting the server machine as its LAN proxy on the default port 80 (see Figure 12).

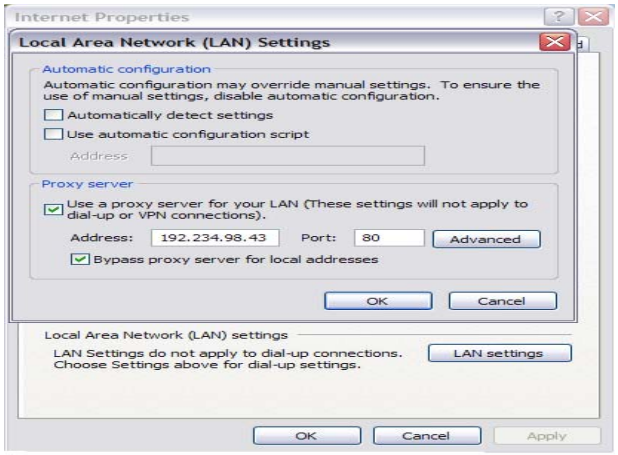

Fig 12. The Internet Explorer's LAN settings

IV. DISCUSSION

A. *Advantages and Limitation*

Applying the APTIPWD to a proxy based computer network has advantages and limitations. The advantages can be summarized as follows:

1. It is easy to implement. There is no need to write any programming code.
2. It is a browser independent tool. Thus, there is no specific browser that is required for the tool to be run.

[5] Computer network settings in Durham University. Available at: http://www.dur.ac.uk/its/services/network/lan/quicksettings, last access on 2 December 2008.

3. Since the training is sent by email, the Administrator is able to send anti-Phishing training to specific users.
4. The aim of training users without informing them that it is anti-Phishing training is satisfied.
5. The aim of training users while they normally use the Internet is satisfied.

In contrast, a possible limitation of applying the APTIPWD to a proxy based computer network is that because the network proxy is added with new tasks to perform (i.e. checking the fixed list of anti-Phishing training websites (FLAPTW) when a URL request is received), the proxy speed for handling the requests might slow down. However, when the APTIPWD has few anti-Phishing training websites, then the checking process does not consume much time. In the APTIPWD prototype, there were eleven URLs that needed to be checked. This did not cause a noticeable slow down to the speed of the traffic.

B. Deploying the APTIPWD with its own Proxy in a Proxy based Computer Network

Applying the New Approach (APTIPWD) to an existing proxy based computer network has been described. This means that the proxy used in applying the APTIPWD is the network proxy that handles the URLs requests made by the network's clients. The proxy needs to be configured to communicate with the Apache HTTP Server and the clients.

In addition to this, the APTIPWD can be applied to a proxy based computer network (in this instance, Durham University network) without configuring its proxy. This was accomplished by having a proxy only for running the APTIPWD. This meant that there were two proxies when the APTIPWD was running; the Durham University network's proxy and the APTIPWD's own proxy. The APTIPWD's proxy was planted between the Durham University network's proxy and the Client. For this to be done, a simple alteration to the Apache HTTP Server configuration file, shown in Figure 8, was performed. As presented in Figure 13, the APTIPWD's proxy forwarded all URLs requests to the University proxy unless the URLs requested were listed to be served in the APTIPWD local server.

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule cache_module modules/mod_cache.so
LoadModule disk_cache_module modules/mod_disk_cache.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so


<IfModule mod_proxy.c>
ProxyRequests On
AllowCONNECT 80 443
<Proxy *>
Order deny,allow
Deny from all
Allow from 192.168.1.65
</Proxy>
</IfModule>



ProxyRemote  *  http://wwwcache.dur.ac.uk:8080
NoProxy         www.ebay-security.com www.paypa1.com www.online.llOydstsb.co.uk www.amazon.co.uk.me.com
```

Fig 13. Pointing the Durham University's proxy in the Server's configuration file

V. CONCLUSION

In this paper, an approach to the implementation of the anti-Phishing training intervention for Phishing websites detection (APTIPWD) was presented. The APTIPWD presents an intervening message to users who access Phishing websites and try to submit their information. The intervention message uses the most effective anti-Phishing tip evaluated in a previous study [10]. By using this approach, users do not need to attend training courses and do not need to access online training materials. This is because the approach brings information to end-users and helps them immediately after they have made a mistake in order to detect Phishing websites by themselves.

The paper discussed the advantages and the possible limitation of the APTIPWD. It also showed that the APTIPWD is feasible and can be implemented easily without writing a single line of a programming code and without undue disruption of the users system.

Future work will attempt to implement and apply the APTIPWD to the real Internet using dynamic anti-Phishing blacklists that are updated continuously.

REFERENCES

[1] S. Philippsohn, "Trends In Cybercrime — An Overview Of Current Financial Crimes On The Internet", in *Computers & Security*, 20 (1), 2001 pp. 53-69.

[2] CyberSource, "9th Annual Online Fraud Report", Edition: 2008 [online]. Available: http://www.cybersource.com, last access on 20/3/2007.

[3] 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.

[4] M. Chandrasekaran, R. Chinchani and S. Upadhyaya, "PHONEY: Mimicking User Response to Detect Phishing Attacks". Proc. International Symposium on a World of Wireless, Mobile and Multimedia Networks. Washington DC: IEEE Computer Society, 2006, pp. 668-672.

[5] A. Litan, "The War on Phishing Is Far From Over", Report: 2009 [online]. Gartner Group. Available: http://www.gartner.com/DisplayDocument?ref=g_search&id=927921, last access on 25 June 2009.

[6] 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.

[7] Symantec, "Mitigating Online Fraud: Customer Confidence, Brand Protection, and Loss Minimization", 2004 report [online]. Available: http://www.antiphishing.org/sponsors_technical_papers/symantec_online_fraud.pdf, last access on 21/3/2007.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] Microsoft Corporation, "Microsoft Security for Home Computer Users Newsletter" [online]. Available: http://www.microsoft.com/protect/secnews/default.mspx, last access on 16 March 2007.

[13] 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.

[14] 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.

[15] W. Jia, and W. Zhou, *Distributed Network Systems: From Concepts to Implementations*. New York: Springer, 2004.

[16] M. P. Singh, *the Practical Handbook of Internet Computing*. USA: Chapman & Hall/CRC Publisher, 2005.

[17] Y. Xiao and H. Chen, *Mobile Telemedicine: A Computing and Networking Perspective*. USA: Auerbach Publications, 2008.

[18] Apache. "Apache HTTP Server Project" [online]. Available: http://httpd.apache.org, last access on 1 December 2008.

[19] Apache, "Apache Virtual Host documentation" [online]. Available: http://httpd.apache.org/docs/2.0/vhosts, last access on 1 December 2008.

[20] A. Friedlander, A. Mankin, W. D. Maughan and S. D. Crocker, "DNSSEC: a protocol toward securing the internet infrastructure", in *Communications of the ACM*, 50 (2), 2007, pp. 44-50.

[21] Maktoob mail portal [online]. Available at: http://mail.maktoob.com/login.php, last access on 10 August 2008.