Improved Awareness on Fake Websites and Detecting Techniques

Hossein Jahankhani, Thulasirajh Jayaraveendran, and William Kapuku-Bwabw

School of Computing, Information Technology and Engineering
University of East London, UK
h.jahankhani@uel.ac.uk, thulasirajh@gmail.com,
wbkapuku@yahoo.co.uk

Abstract. Fake website pages use the similar page layout, font style and picture to mimic legitimate web pages in an effort to convince internet users to give their personal sensitive information such as bank account number, passwords, personal details etc and also sell fake products like fake ticket, duplicate brand cloths, medication etc. There are many available techniques in the market to identify the fake websites. This paper provides an efficient awareness on detecting fake websites. A novel technique or tool will be proposed, implemented and analysed. This technique visually compares a suspected fake website page with legitimate web page by capturing the snapshot of the fake page and identifies it using the assigned identity pixels which are in the legitimate webpage.

Keywords: cybercrime, scammers, fake websites, URL.

1 Introduction

Fake website is one form of phishing, usually scammers create a fake website whose appearance is similar to the page of a real website in order to trick the internet users to divulge their credentials and identities which scammers will use to commit identity theft and fraud for instance they may open bank accounts, take credits from financial institutions etc. also the scammers are able to sell their fake products. Perpetrators of fake websites always use the current or seasonal trend of business. For Example scammers create a fake website and sold fake tickets to the top sporting and entertainment events.

It is obvious that there are lots of computer and internet users who lack online security skills and are not aware of fake websites; hence they would easily fall into the scammers trap. Once they enter their personal sensitive information into a fake website, this information is used by fraudsters for illegal transactions [9] in their article “Bank to rights, we smash dodgy migrant's £1m credit card racket” stated that recently in East London a man was arrested for fraud by Met Police. The detainee person used websites to acquire victim’s credit cards information and illicitly use or sell them. Furthermore, nowadays websites are powerful media which easily assist people to communicate with others and facilitate people to perform transactions online. It is noticeable that rumors are quickly created and easily spread to the public

H. Jahankhani et al. (Eds.): ICGS3/e-Democracy 2011, LNICST 99, pp. 271–279, 2012.

via fake websites. In the light of all the above, it is obviously that fake websites effectively causes concerns for law and public order. The research has noticed that the followings major factors:

- Lack of user awareness regarding online security
- Authentic design of the fake websites (high quality and professional designing)
- The belief by some victims that the law enforcement agencies will not act if they report computer-related crime.
- Lack of education in online security
- It is easy and cheap to create a fake websites
- Individuals are scared and reluctant to report incidents to the police through embarrassment.

2 Background

The method of crime is shifted from traditional methods to electronic methods. Hence this has turned out to be a biggest challenge issue to the modern world especially to the law enforcement agencies. Thus it is imperative to find an effective solution to eradicate this growing virtual method of committing crimes which is cybercrime. There is considerable debate surrounding what the term 'cybercrime' means. The Association of Chief Police Officers (ACPO) has recently defined e-crime as 'the use of networked computers or Internet technology to commit or facilitate the commission of crime" [1].Cybercrime is a crime that takes place within cyber space, which could be said to represent the virtual environment within which networked activity takes place [17]. According to surveys, the scale and the volume of the crimes are too large so technical complexities make almost impossible to identify the criminals, since there is a large volume of data to be scanned to identify perpetrators and bring them to justice. Cyber criminals have the belief that the implementation and enforcement of the law is difficult in the online world, therefore they perform their illicit acts without any fear.

2.1 Use of Internet

Over the past 15 years there has been an immense increase in internet usage by individuals of all age. According to the report there were 1.97 billion internet users; 475.1 million in Europe and 825.1 million in Asia. The same survey stated that there was over 14% increase from previous year. [12]. Furthermore "www.symbolic.com" was first domain registered in the world in 1985; there were more than 255 million websites on internet and 152 million blogs –net craft's web server survey December 2010[18]. Cyber criminals use complicated Fake website technical methods when designing fake websites. And these methods are really hard to detect. Some of the methods are:

- Add suffix to the domain name
- Use the mimic link different from visible link

- Use the redirect bugs to redirect the link to the fake pages.
- Replace the certain characters in target URL with similar characters [3]
- Cover the address bar to scam users into believing they are in correct page. It is achieved by adding some script or image to fake the address bar.
- Use the visual based content like image, flash, java applet.
- Use the downloaded WebPages from the real website to make the fake web pages which appear and react exactly as the legitimate web pages.

This paper is attempts and intends to answer the following research question: How best can the public and law enforcement agencies detect fake websites? For examples; in august 2008, Olympic game was held in china, for those games some of the websites sold fake tickets. For instance this site http://www.beijingticket.com was selling fake tickets and committing fraud with other people from all around the world. Reports said that the people who have bought tickets from this website are mostly from America, Australia, New Zealand, Britain etc. Furthermore on this website rate of opening ceremony of Olympic were $1750 to $ 2150. This website named http://www.beijing-ticket2008.com was also closed on 23rd July 2008. It is reported that there are many fake websites offering tickets regarding of Olympic Tickets [19]. There is a highly lucrative market for ticketing; scammers are becoming sophisticated, using encryption on fake websites to lure the potential purchaser into a false sense of security. (BBC News, 4 March 2011) [8]. The HM Revenue and Customs (HMRC) has provided some details about the fake web sites so that the consumer may be aware of those and can act accordingly of fake web sites is found .generally the phishing sites target the personal details of the consumer and using those personal details they may go for gaining some profits in improper way, so this leads to theft and fraud [20]. Website www.uk-tiffancyonline.com,which advertised 85% offer. And that site exactly looks like the original tiffancy.com site, and also scammer put this fake site on the Google ad sense. So Google can be paid £5 every time user clicks on that link [7]. Financial institutions and their customers remained the target of phishing attacks over half the time, according to the report. Other specific attack targets included auctions, online payments and government organizations. The top countries for phishing URLs are Romania at 18.8%, the United States at 14.6%, China at 11.3%, South Korea at 9.8% and the United Kingdom at 7.2%. In tracing the origin of phishing emails, IBM research shows India is tops at 15.5%, Russia at 10.4%, Brazil at 7.6%, U.S. at 7.5% and Ukraine at 6.3%. [5, 13]. “Top countries hosting phishing URLs and top targeted sectors in EMEA” - Symantec Corporation [13]. “11% of the online British population has been a victim of online identity fraud in the last 12 months.” - YouGov survey, March 2010 [10]. “1 in 5 businesses has been a victim of an internet scam”. “Over a quarter of UK internet users are more afraid of being a victim of online crime than they were 12 months ago”.-Get Safe Online Report, 2008 [14].

2.2 Fake Website Spreading Techniques

There are so many ways follow by the scammers to spread their fake website into the internet .some of them are:

Semi-Fake Websites: Cyber criminals place a fake popup window in the legitimate website, when a customer accesses the legitimate website; the fake window popup then appears on the body of the legitimate website requesting user to enter his/her details.

Tab Nabbing: Tab nabbing is another technique which is used to launch a fake website. This gathers the user's frequent visits to web pages by means of CSS history mining. And then uses little bit of JavaScript to create a multiple tabs and launches the fake web page in one of the tab. As the user scans their tabs, the fake web tab acts as a strong visual cue memory making the user to simply open that tab and provides their credential in the fake webpage [4].

Evil-Twins Technique: This is method of launching fake website is the very hard to detect. Cyber criminals create a fake website and wireless network that looks similar to the public network, then they establish the network near the coffee shop, hotels etc. Whenever an ordinary user accesses their network, cyber criminals capture his/her sensitive details into a fake website which was hosted in the fake wireless network.

URL Tricking: Cyber criminal registers a fake website with a similar name of a legitimate website to trick the user to disclose hi/her classified data into a fake webpage. For instance, HSBC Bank has customer's transaction site as "http://instancebanking.hsbc.com", cyber criminals have also set up a server using any of the below similar names to obfuscate the real destination host "http://instancebanking.hsbcc.com or http://instancebanking.hssbc.com".

Sub Domain Concept: Some fake websites are registered with the domain name as similar as the legitimate websites domain name. For example, Barclays bank received the phishing scam which used domain name "http://www.barclayze.co.uk". Other examples include using a sub-domain such as "http://www.barclays.validation.co.uk", where the actual domain is "validation.co.uk" which is not related to Barclays Bank as described by Fraud Watch International [6]. Consider this site http:/unibank.onlinebankingcenter.com (Fig.1).

Legitimate website: "http:// www.unibankghana.com";

Fake Website: http://www.unibank.onlinebankingcentre.com [21]

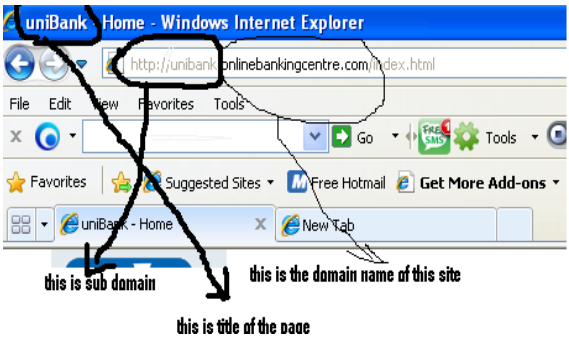

Fig. 1. Sub domain concept

In this page original domain name is onlinebankingcenter.com, sub domain is Unibank and title of the page also Unibank. At a glance, people would think that is a legitimate page of the UNIBANK. Sub domain is the one of the part of main domain, no need of registration required for adding sub domain to the exiting domain. Sub domain and domain is separated by a single dot (.). Scammers utilise this feature and make a fake website in this format. New versions of the browsers are clearly display the URL of the page in the address bar. User easily point out the difference of the domain and sub domain. The fake has a tab for open an account that lead to a form.

URL Encoding Method: Using the "@" symbol to confuse the user, for example login URLs are allowed for the complex URLs to include authentication information such as a login name, passwords. Generally such information is achieved in the format "http://username:password@hostname/pathof the domain page." scammers have a chance to substitute the password and user ID fields for detail associated with the concern. Sample model: **http://hsbc.com:instancebanking@internatiional.com/login.htm** Here, scammers used the login URL concept to mimic the user. Hsbs.com is used as user ID and instance banking used as password and scammers substitute the respective fields. Scammers successfully attract many users into their site, because users think that they are actually visiting a legitimate page. In order to avoid this method, users should use the new version of the browsers and also trusted browsers.

Host Naming Tricks: Most of the internet users are familiar with the fully qualified domain name to navigate to the required websites but at the back of this scene there is a process of converting such domain name to IP addresses. Scammers utilised this feature and obfuscate the destination address and by pass the content filtering server. For example URL: http://hsbc.com:instancebanking@internatiional.com/login.htm. Could be entered as: http://hsbc.com:instancebanking@207.10.10.95/login.htm.

2.3 Use Legitimate Website's Content for Fake Web Page

When analysing the objects of the suspected page, scammers often used the objects from legitimate site, for example, they use a picture, flash objects, streaming videos etc.. Most of the scammers create a frame in the web page and simply link to the legitimate domain. That web page looks like a real web page. But fake website only contains a home webpage and pages such as about us and contact us. This means that fake websites often contain hyperlinks that links to legitimate web site (domain is different from one page to another) [16].

In this case, scammers used the most popular and trusted company logo. Also they provide some tips to detect fake websites, and then users believe that the site they visit is legitimate as they are provided with tips to spot a fake websites. To confirm their details it is advisable not to click on the link provided for verification, users have to visit the trusted network company sites (ABTA, IATA and VERISIGN) and from that site verify the suspected site [6].

URL Spoofing of Address Bar: This method involves removal of the original address bar and then introducing the fake address bar with the help of images and

texts. the link is send to a legitimate user through e-mail and when the user clicks on the link it will open a new browser window, which closes and re-opens without the address bar, sometimes status bar, The new window uses HTML, HTA and JavaScript commands to construct a false address bar in place of the original. In order to avoid this cyber attack: since it uses scripts it can be able to stop by disabling active x and java scripts in browser settings.

To Avoid Scam Websites:

- User should be more careful before entering into payment by noting the letters "https" on the web address.
- Buy from trusted pages which were linked from official web pages,
- A sponsored link on a search engine or other website offers no guarantee of authenticity (Sunday times, 2010) [7]
- Spend more time to analyse a suspicious website before making any transactions.
- Look for UK limited company details and a VAT number, if one, or both are absent, this may raise suspicions
- Go to the WHOIS website and check the status and registered details of that page (don't click any link says "who is look up" from the same website)
- Some fake whois website also available in internet.
- If more tabs are open in browser means, don't do any transaction, close all the tabs whichever not necessary at that time and do the transaction.
- Don't leave any credential data request/access page inactive for long time. And also don't access the page if it has inactive for a long period.
- Always check the address bar, whether it shows known domain name, don't do any transaction if there is suspicious URL.
- @, more (.), - symbol found means be alert and verify other factor to ensure that site is legitimate [13,6,8].

3 Implementation of Proposed System

3.1 Proposed System

The improved toolbar is proposed for the purpose of providing awareness regarding a fake website and also differentiating a fake website from legitimate website (fig.2). The system proposes three different levels of detection process involved in detecting a fake website:

Level 1 (Minimal) - URL Identity Check: This level of protection will check URL itself and advise whether it is legitimate or not. This check is achieved by analysing suspected symbols in the URL (for example '@' more dot (.) symbols). This level is very basic.

Analyse the URL and display the URL to the user- this creates user awareness. User is able to identify the URL. Fake address bar and other URL will be cleared in this level of detection. Message box clearly displays the original link which the user is visiting at that time.

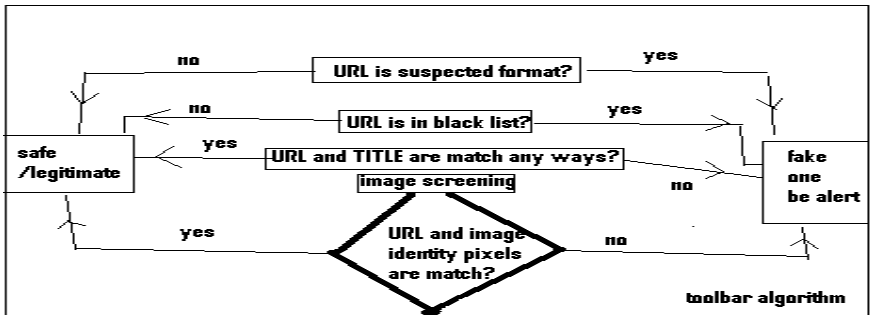

Fig. 2. Improved toolbar is proposed

Level 2 (Medium)-Black List Check: This level of protection will check the list of black list and white listed base for fake website URL. If URL is in the black list, it will show the warning to user as fake site. (Black list are obtained from the common anti-phishes database). Additionally at this level, tool will compare the title of the webpage and the URL, if anything is suspicious the system will alert the user.

To perform this test we have to maintain two data base column, black list and white list. Data base tables have to be updated periodically and the black list information may be gathered from some of the site monitoring forum. In the case of new sites which are not in both lists, there will be a massage box alerting the user to do further investigations on a suspected site.

Additionally compare the URL on the address bar and title of the webpage, if URL is completely different from the title of that page then massage box will alert the user as "page title and URL doesn't match – site may be suspicious".

Level 3 (Maximum) - Image Based Screening: The system captures the current page and checks the image pixel with the already stored pixels. If the pixels are matched with the database pixel for the given URL then that one is legitimate. If it is not then tool will alert the user. For a better result of this detection, the secure pages should be designed with various identity points (pixel) all over the page, so identity pixels contain little colour difference than adjacent pixels. (Example: page with white background and colour value for white is 00000, then identity point's colour value is 000001).

At this level, a database stores the identity pixels detail of the webpage and updates the pixel information periodically, below we use the windows application to update the pixel information to the database. This application is designed for the purpose of updating the pixel information to the database. This application captures the screen short of the webpage by means of buffer memory and then picks the pixel from that image (fig.3).

While performing the level 3 detection, client side webpage will convert as image and particular pixels will be taken from that webpage image (client side) and compare against pixels stored in a database. If there is match in the identity pixels in a URL, this means that image belongs to that URL. A message will be displayed as "current loaded page is legitimate" otherwise the display massage will show "current loaded page is fake".

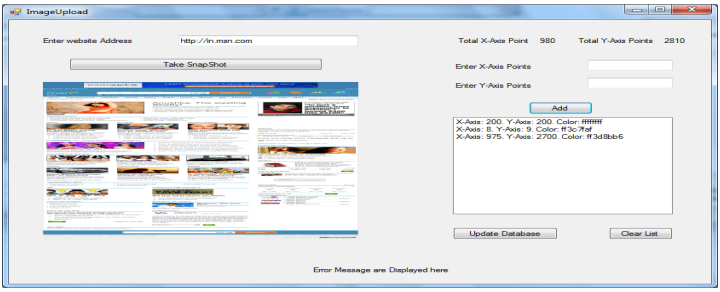

Fig. 3. Shows image based screening with different colours

4 Conclusion

This paper provides an efficient awareness in detecting a fake website. Providing concept of fake website and its spreading method itself creates a big awareness among the internet users. No matter what security measures fitted in a device to protect online information, users should be regularly made aware of new approach to fight cyber crimes. In this paper we have attempted and intended to propose, implement and analyse a new improved tool which assists to detect fake website. Furthermore it creates the awareness on fake website detection.

References

1. http://www.acpo.police.uk/asp/policies/Data/Ecrime%20Strategy%20Website%20Version (accessed October 17, 2010)
2. Amoo, D.I.P., Thomson, N.: ACPO e-crime Strategy, Version 1.0 ACPO, the Association of Chief Police Officers of England, Wales and Northern Ireland, e-Crime Strategy (2009)
3. Fu, A.Y., Deng, X., Liu, W.: A Potential IRI Based Phishing Strategy. In: Ngu, A.H.H., Kitsuregawa, M., Neuhold, E.J., Chung, J.-Y., Sheng, Q.Z. (eds.) WISE 2005. LNCS, vol. 3806, pp. 618–619. Springer, Heidelberg (2005)
4. http://www.azarask.in/blog/post/a-new-type-of-phishing-attack
5. Messmer, E.: 31.03.2011 kl 22:52 | Network World (US), http://news.idg.no/cw/art.cfm?id=90A7235F-1A64-6A71-CEF6A16B1DEE1DC1
6. http://www.fraudwatchinternational.com/phishing-fraud/phishing-web-site-methods/#content
7. Internet bank fraud statement, Sunday times (January 09, 2010), http://www.met.police.uk/fraudalert/docs/internet_bank_fraud.pdf
8. http://news.bbc.co.uk/1/hi/uk/8189905.stm
9. News of the world (2011), http://www.newsoftheworld.co.uk/notw/_news/1280300/Webcatch-Nigerian-crime-boss-who-cons-Brits-out-of-millions-of-pounds-each-year-online.html

10. YouGov survey commissioned by VeriSign Authentication, Cifas report (March 2010)
11. Phishing Activity Trends Report-APWG Q1/2010
12. http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers
13. Symantec Corporation report, http://www.nortoninternetsecurity.cc/2011/04/symantec-internet-security-threat.html
14. UK Internet Security: State of the Nation - Get Safe Online Report (November 2008), http://www.getsafeonline.org/media/GSO_Report_2008.pdf
15. http://www.velocityreviews.com
16. http://www.wiki-news.com/fakewebsites
17. Wall, D.S.: Cybercrime: Transformation of crime in the information age. Polity Press, Cambridge (2008)
18. web server survey (December 2010), http://news.netcraft.com/archives/2010/12/01/december-2010-web-server-survey.html
19. Amit ranat, http://www.groundreport.com (August 07, 2008)
20. Simon frediction, http://www.shopsafe.co.uk (August 16, 2010)
21. http://www.unibank.onlinebankingcentre.com