Study of Cloned Websites: Practical View of Phishing Website Design and Prevention

Arun Anoop M

PhD Scholar(Anna University, Chennai),
Reg no: 1615479206
Dept. of Computer Science & Engineering,
Velammal College of Engineering & Technology,
Madurai,TamilNadu,India

Abstract - Cloned website creation is one of the serious threat in Wireless network or internet. The password stealing of humans is done by the hackers mostly through internet. Nowadays internet is not so safe. Many cyber cases reported recently based on bad or illegal activities. Safety on humans is not guaranteed. Likewise nothing is safe in internet. There is no guarantee in that also. Many of the hackers were created cloned websites and they are mapping ip address with the website name with the help of dns spoofing. There are plenty of softwares available in market to make an URL that start with https. In this paper we propose a phishing website creation with the help of Kali Linux social engineering toolkit. After the creation of cloned website , use existing anti phishing tools to detect and prevent the phishing websites. Prevention method mainly focused on existing web browser plugins . Toolbars, online websites for anti phishing, Online game for anti phishing. And finally will do an analysis work on it. Our work mainly focused on vmware virtual workstation and on my client_ PC. Cloned website created in Kali Linux(VM ware). Detailed analysis work will be the core part of the work.

***Keywords* - Cloning, Phishing, Anti Phishing, DNS Spoofing, Password Stealing, Kali Linux, Spoofing, Wireless Network, Social Engineering.**

1. Introduction

The Internet is playing a significant role in today's life. We can see the definition of phishing in different way of presentation:

Phishing, a method of online identity theft[1]. In addition to stealing personal and financial data phishers can infect computers with the help of viruses and convince people to participate in money laundering[1]. Phishing is an activity usually made through email to steal personal information[2]. The best way to protect yourself from phishing is to learn how to recognize a phishing[2]. Phish Tank is a collaborative clearing house for data and information about phishing on the Internet[3]. Also PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no cost[3]. Phishing is an e-mail fraud method and it is an attempt to gather personal and financial information from recipient[4]. Phishing is a type of e-mail scam implemented to steal your identity[5].

Fraudsters send fake emails or set up fake web sites that mimic Facebook's sign-in pages (or the creation of sign-in pages of other genuine transaction companies such as eBay or PayPal) to trick you into disclosing your user name and password[6]. This is sometimes referred to as phishing. The word fishing the fraudster is fishing for your private account information[6]. There are many social engineering tools available in kali linux.

Phishing attacks use electronic-mail or malicious websites to collect personal and financial information. Sometimes it infect the machine with malware and viruses[7].Anti-Phishing Working Group (APWG) mainly aim to train users on how to prevent themselves from phishing attacks[8].

Phoneybot : Honeypot as a robot against phishing.

VISHING – this is a term which combines voice and phishing. Vishing is defined as when you get a phone call from a legitimate company to verify some personal information about you.

SMISHING – This word is taken from SMS texting and Phishing[23].

Spear Phishing – Phishing attempts directed at specific individuals or companies have been termed spear phishing[20].

Pharming **:** Pharming is that the term given to hosts file modification or name System (DNS)-based phishing[19]. Malware Based Phishing refers to scams that involve running malicious software on users PCs[19].

Session Hijacking malicious software takes over and can undertake unauthorized actions(transferring funds) without the user's knowledge[19]. Web Trojans collect the users credentials locally and transmit them to the phisher[19]. Search Engine Phishing For example scammers have set up false banking sites offering lower credit costs or better interest rates than other banks[19].

Whenever user finds a selected webpage as pretend one then the person will report the phishing on following centers of below:

- Anti-Phishing-Working-Group
- Federal-Trade-Commission
- Internet-Crime-Complaint-Center

There are plenty of online games available in internet (related to phishing scams) to give awareness.In this paper, create a clone website and analyze it with the help of firefox plugin tools. Clone website creation is categorized into two.

- Based on vmware workstation and kali linux
- Based on phish.php and one free host website.

2. Design of Phishing

2.1 Based on Vmware Workstation and Kali Linux

1) Install Kali Linux
2) Application
3) Kali Linux
4) Exploitation Tools
5) Social Engineering Toolkit
6) Click on se-toolkit

Social engineering is a product of TrustedSec. There are many options available.

Source: [22]
Select one option among seven. I selected first option and the steps for the creation (1) Social engineering-attacks(2)Website-attack vendors (3)Credential Harvester Attack method (4)Site cloner. (5) Enter our virtual machine ip address(Use terminal to find ip address with the help of ifconfig utility).

1) Enter ip address.
   192.168.150.128
2) Enter the URL to clone
   Facebook website and followed by login.php
3) It will take time to finish the process. Minimize the virtual machine.
4) Open Web browser in the machine.
5) Type Virtual machine ip address on the address bar. It will show our cloned website.
6) Enter your facebook username and password.
7) Just minimize the web browser to see the virtual machine terminal window to know the status. Listen and watch the traffic.
8) Note down the username and password for future use.

Future Work: Researcher can use `ettercap` dns spoof utility to map ip address with web address.

2.2 Based on Phish.Php and One Free Host Website

Phishing is a way of attempting to acquire information such as username, password and credit card details of persons[1]. Phishing pages created in free webhost is easily report and block by modern tools. But phishing pages created in hosted website is difficult to catch by any powerful tools. Steps

1) Open gmail
2) Save page as `index.html`
3) Within that folder create `phish.php`
4) Create an empty text file named `log.txt`
5) Open `index.html` in notepad
6) Search(use Ctrl+F) to know
   Action=” ” field. Replace body between double quotes with `phish.php`.
7) Create free host website. Example
   000webhost website.
8) Created gmailpasswd.webuda.com
9) Login and delete current `index.html` file from control panel.
10) And upload edited `index.html`
11) Send the faux web site address to victim with any message like “Please modification your gmail positive identification.”

3. Defend against Phishing

In this paper we analyzed ‘existing anti phishing firefox plugins’ to defend against based on vmware workstation and kali linux. Analysis is based on the working of existing anti phishing tools in Firefox web browser.

Table 1:Tools and its sign

Anti-Phishing Tools	*Its sign*
Anti-Phishing 1.0	Not predicting phishing sign
DontPhishMe 1.7.16.2	Not predicting phishing sign
Facebook Phishing Protector 4.4.3	Predicting phishing sign
urlcheck 0.1	Not predicting phishing sign
WorldIP 3.0.8	Not predicting phishing sign
Trust My Web 1.6	Not predicting phishing sign

4. Tools and its Duty

1) Google Safe Browsing: Safe Browsing may be a Google service that allows applications to see URLs against perpetually updated lists of antecedently noted phishing, malware, and unwanted package pages[9]. “Google Safe Browsing” designed to spot dishonorable internet sites.
2) McAfee SiteAdvisor - FREE PLUG-IN: McAfee uses a military of check computers to check the net for everything from spam ,spyware or phishing[10].
3) Netcraft Toolbar: Protect your savings from Phishing attacks[11]. Blocks phishing sites, helping to protect users from online fraud[12].
4) EarthLink Toolbar[13][15]: It helps to
   a. Protect you from online scams.
   b. Online scams try to steal your personal information.
   c. Display a security rating for all Web sites you visit.
   d. It alerting you before you enter a Web site on a known fraud sites list.
5) Cloudmark Anti-Fraud Toolbar: If a link is harmful web page that contains spyware, viruses, worms, identity theft or phishing attacks then the Cloud mark anti-fraud toolbar will detect the URL as "Unsafe" and will block that page from viewing[14].
6) eBay Toolbar with Account Guard[16]:It is a free program that gives you quick access to eBay from anywhere on the Web. Account Guard protects your eBay and PayPal passwords and alerting you if you enter into an unauthorized site.
7) McAfee SiteAdvisor: It alerts users to possible phishing and identity theft scams[17].
8) GeoTrust’s TrustWatch Toolbar: It alerts you to unsafe or “phishing” web sites [18]. Phishing websites can steal private information and lead to identity theft.
9) Anti Phishing Phil Game: Anti Phishing Phil Game: Anti-Phishing Phil is an alternate bold that teaches users how to analyze phishing URLs from counterfeit websites[21].

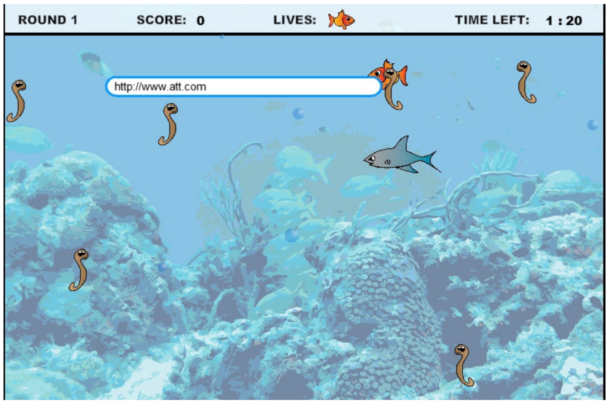


Fig. 1. Genuine Website[25]

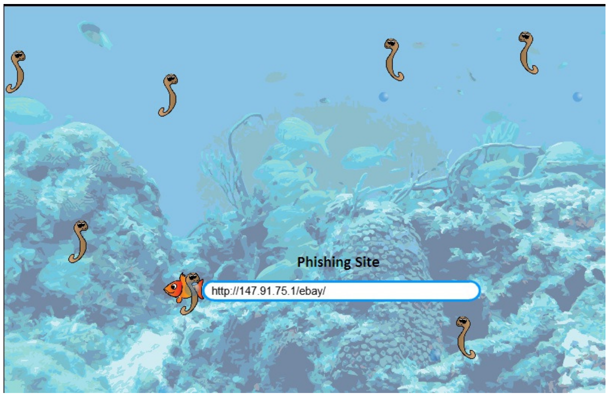
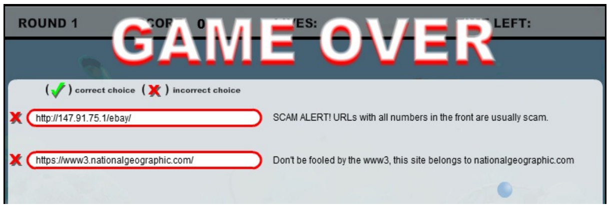


Fig. 2. Phishing Website[25]



✗ http://147.91.75.1/ebay/ SCAM ALERT! URLs with all numbers in the front are usually scam.

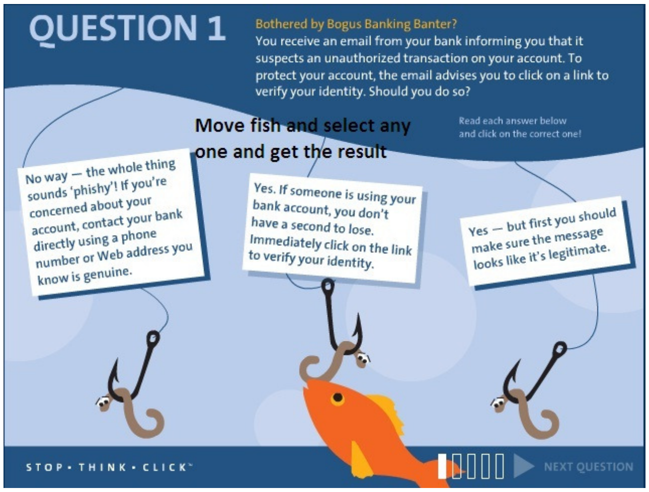
✗ https://www3.nationalgeographic.com/ Don't be fooled by the www3, this site belongs to nationalgeographic.com

Fig. 3. Result

Website_source:
[24-25]

10) phishing-scams game:
Source:[26]

Download **phishing_game_source.zip**
And Open and see the game.



QUESTION 1

Bothered by Bogus Banking Banter?

You receive an email from your bank informing you that it suspects an unauthorized transaction on your account. To protect your account, the email advises you to click on a link to verify your identity. Should you do so?

Read each answer below and click on the correct one!

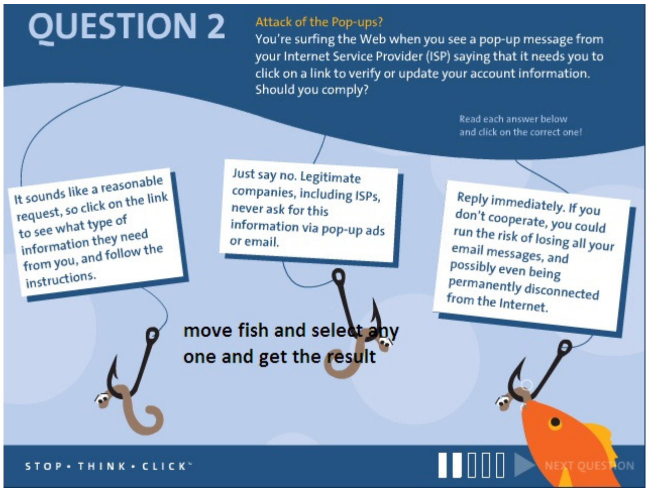
Move fish and select any one and get the result

No way — the whole thing sounds 'phishy'! If you're concerned about your account, contact your bank directly using a phone number or Web address you know is genuine.

Yes. If someone is using your bank account, you don't have a second to lose. Immediately click on the link to verify your identity.

Yes — but first you should make sure the message looks like it's legitimate.

Fig. 4. Question 1[25]



QUESTION 2

Attack of the Pop-ups?

You're surfing the Web when you see a pop-up message from your Internet Service Provider (ISP) saying that it needs you to click on a link to verify or update your account information. Should you comply?

Read each answer below and click on the correct one!

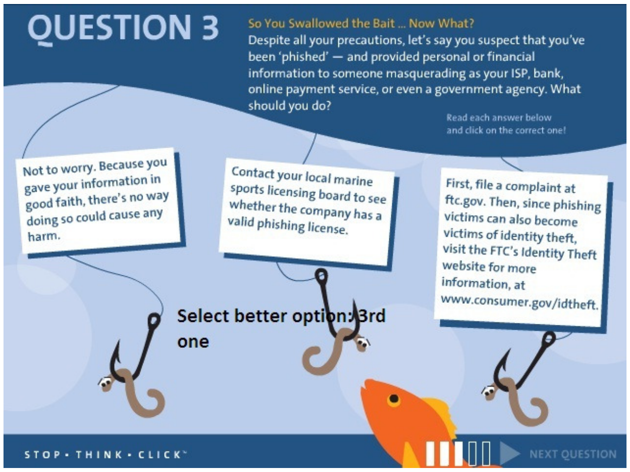
It sounds like a reasonable request, so click on the link to see what type of information they need from you, and follow the instructions.

Just say no. Legitimate companies, including ISPs, never ask for this information via pop-up ads or email.

Reply immediately. If you don't cooperate, you could run the risk of losing all your email messages, and possibly even being permanently disconnected from the Internet.

move fish and select any one and get the result

Fig. 5. Question 2[25]



QUESTION 3

So You Swallowed the Bait ... Now What?

Despite all your precautions, let's say you suspect that you've been 'phished' — and provided personal or financial information to someone masquerading as your ISP, bank, online payment service, or even a government agency. What should you do?

Read each answer below and click on the correct one!

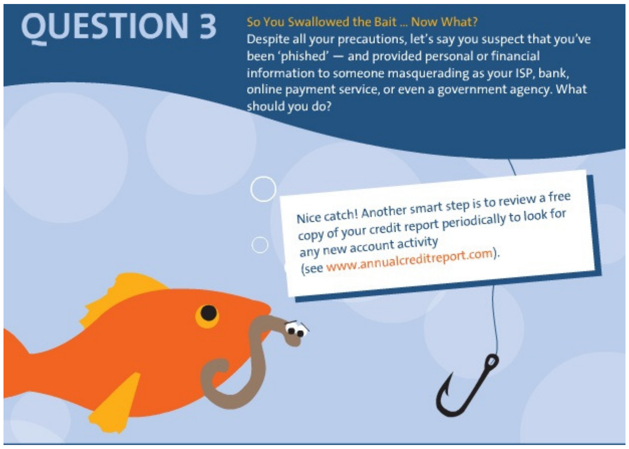
Not to worry. Because you gave your information in good faith, there's no way doing so could cause any harm.

Contact your local marine sports licensing board to see whether the company has a valid phishing license.

First, file a complaint at ftc.gov. Then, since phishing victims can also become victims of identity theft, visit the FTC's Identity Theft website for more information, at www.consumer.gov/idtheft.

Select better option: 3rd one

Fig. 6. Question 3[25]



QUESTION 3

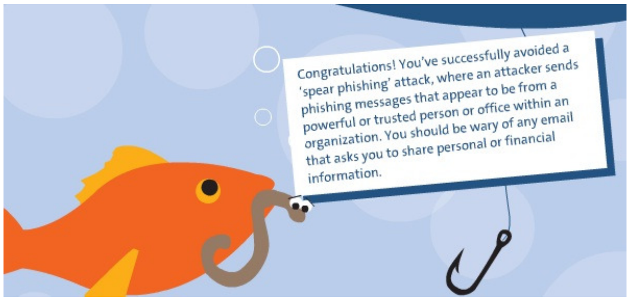
So You Swallowed the Bait ... Now What?

Despite all your precautions, let's say you suspect that you've been 'phished' — and provided personal or financial information to someone masquerading as your ISP, bank, online payment service, or even a government agency. What should you do?

Nice catch! Another smart step is to review a free copy of your credit report periodically to look for any new account activity (see www.annualcreditreport.com).

Fig. 7. Final option[25]

Question 4 select the first option to avoid spear phishing attack.



Congratulations! You've successfully avoided a 'spear phishing' attack, where an attacker sends phishing messages that appear to be from a powerful or trusted person or office within an organization. You should be wary of any email that asks you to share personal or financial information.

Fig. 8. Spear Phishing attack[25]

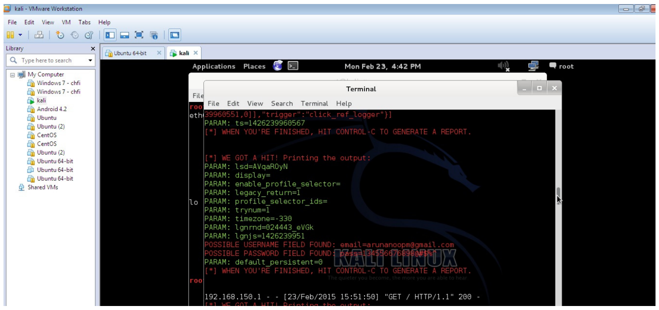
What to do about messages that ask for your personal information.
Source:https://www.onguardonline.gov/topics/avoid-scams

11) SonicWALL Phishing IQ Test:

Source:
http://www.sonicwall.com/furl/phishing/phishing-quiz-question.php

5. Working Analysis

Kali Analysis Result based on 2 A.,



```
39960551,0]],"trigger":"click_ref_logger"}]
PARAM: ts=1426239960567
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


[*] WE GOT A HIT! Printing the output:
PARAM: lsd=AVqaROyN
PARAM: display=
PARAM: enable_profile_selector=
PARAM: legacy_return=1
PARAM: profile_selector_ids=
PARAM: trynum=1
PARAM: timezone=-330
PARAM: lgnrnd=024443_eVGk
PARAM: lgnjs=1426239951
POSSIBLE USERNAME FIELD FOUND: email=arunanoopm@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=134556676898@#$%^
PARAM: default_persistent=0
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.150.1 - - [23/Feb/2015 15:51:50] "GET / HTTP/1.1" 200 -
```

Fig. 9. Kali Linux Analysis Output

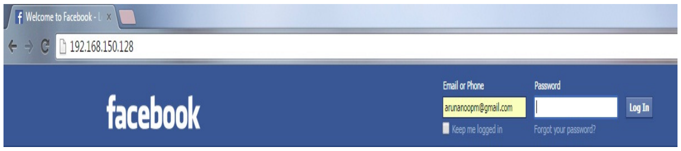
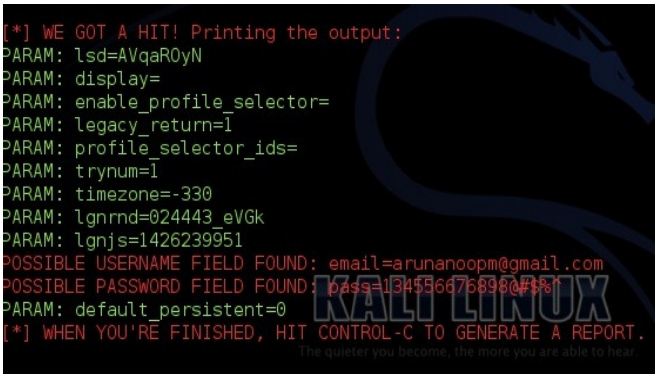


Fig. 10. Cloned Facebook Page

Ip address of VM_ware machine is 192.168.150.128

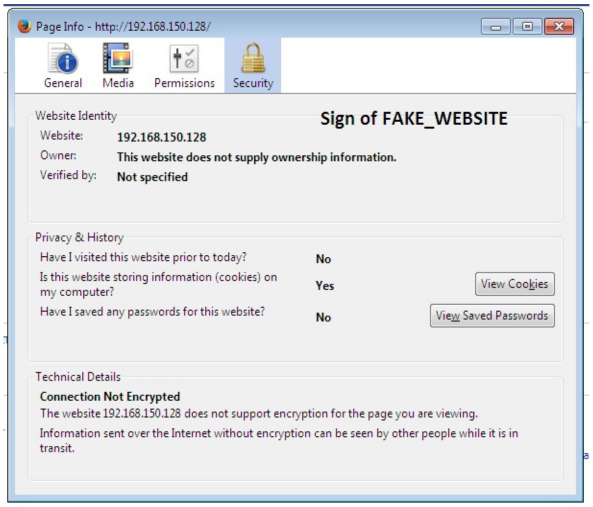


```
[*] WE GOT A HIT! Printing the output:
PARAM: lsd=AVqaROyN
PARAM: display=
PARAM: enable_profile_selector=
PARAM: legacy_return=1
PARAM: profile_selector_ids=
PARAM: trynum=1
PARAM: timezone=-330
PARAM: lgnrnd=024443_eVGk
PARAM: lgnjs=1426239951
POSSIBLE USERNAME FIELD FOUND: email=arunanoopm@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=134556676898@#$%^
PARAM: default_persistent=0
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Fig. 11. Analysis Output

III. Analysis based on Facebook Phishing Protector 4.4.3

1. Sign of Fake websites:



Page Info - http://192.168.150.128/

Sign of FAKE_WEBSITE

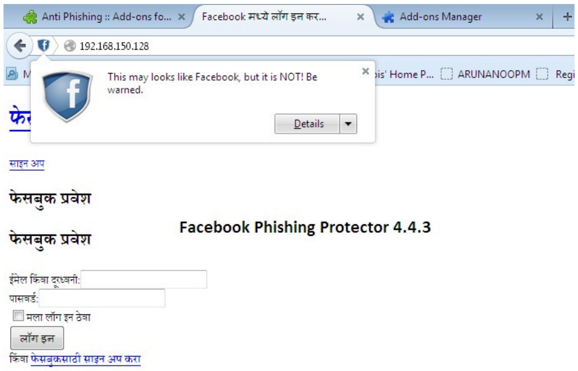
Website Identity
Website: 192.168.150.128
Owner: This website does not supply ownership information.
Verified by: Not specified

Privacy & History
Have I visited this website prior to today? No
Is this website storing information (cookies) on my computer? Yes [View Cookies]
Have I saved any passwords for this website? No [View Saved Passwords]

Technical Details
Connection Not Encrypted
The website 192.168.150.128 does not support encryption for the page you are viewing.
Information sent over the Internet without encryption can be seen by other people while it is in transit.

Fig. 12. Sign of Fake websites

2.



This may looks like Facebook, but it is NOT! Be warned.

साइन अप

फेसबुक प्रवेश

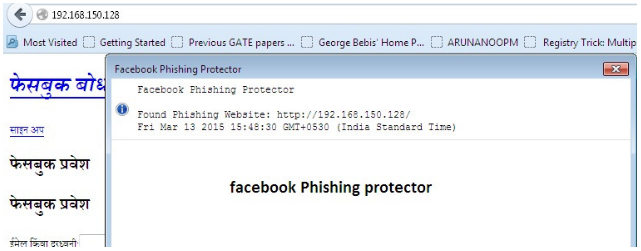
फेसबुक प्रवेश

Facebook Phishing Protector 4.4.3

ईमेल किंवा दूरध्वनी:
पासवर्ड:
□ मला लॉग इन ठेवा
लॉग इन
किंवा फेसबुकसाठी साइन अप करा

3.

Fig. 13. Facebook Phishing Protector Analysis



Facebook Phishing Protector

```
Facebook Phishing Protector

Found Phishing Website: http://192.168.150.128/
Fri Mar 13 2015 15:48:30 GMT+0530 (India Standard Time)
```

facebook Phishing protector

Fig. 14. Facebook Phishing Protector Analysis final

6. Conclusion

We had given brief idea about phishing, its design and had mentioned some important tools to defend against phishing. We mentioned design phase based on kali linux and webhost. After that we analyzed existing antiphishing plugins -tools based on its performance. In future, researchers can do dns spoofing to map ip address with web address.

Acknowledgments

The author thank the anonymous reviewers for their insightful comments and helpful suggestions.

References

[1] Phishing, Available: http://computer.howstuffworks.com/phishing.htm

[2] Phishing,Available: https://www.phishtank.com/what_is_phishing.php

[3] Phishing,Available:https://www.phishtank.com/index.php

[4] Phishing,Available: http://searchsecurity.techtarget.com/definition/phishing

[5] Phishing,Available: http://www.microsoft.com/security/online-privacy/phishing-scams.aspx#Recognize

[6] Phishing,Available: https://safety.yahoo.com/Security/PHISHING-SITE.html

[7] Phishing,Available: https://www.staysafeonline.org/stay-safe-online/keep-a-clean-machine/spam-and-phishing

[8] Srishti Gupta, Ponnurangam Kumaraguru, Indraprastha Institute of Information Technology, Delhi," Emerging Phishing Trends and Effectiveness of the Anti-Phishing Landing Page",June 2014.

[9] Safe Browsing, Available: *https://developers.google.com/safe-browsing/*

[10] McAfee SiteAdvisor - FREE PLUG-IN, Available: *http://www.siteadvisor.com/download/windows.html*

[11] Net Craft toolbar, Available:*http://toolbar.netcraft.com/*

[12] Net Craft toolbar plugin, Available: *https://addons.mozilla.org/en-us/firefox/addon/netcraft-toolbar/*

[13] EarthLink_Toolbar,Available: *http://www.tucows.com/preview/359635/EarthLink-Toolbar-For-Internet-Explorer*

[14] Cloudmark_Anti-Fraud_Toolbar,Available: http://www.tacktech.com/news.cfm?subtype=tech&nid=6074

[15] EarthLink_Toolbar,Available: http://www.earthlink.net/software/domore.faces?tab=toolbar

[16] eBay Toolbar,Available:*http://download.cnet.com/eBay-Toolbar/3000-12512_4-10153544.html*

[17] McAfee_SiteAdvisor,Available: *https://www.siteadvisor.com/final/index.html*

[18] GeoTrust's_TrustWatch_Toolbar,Available: *https://www.geotrust.com/comcasttoolbar/*

[19] PC world Article,Available: *http://www.pcworld.com/article/135293/article.html*

[20] Phishing,Available: *http://en.wikipedia.org/wiki/Phishing*

[21] Anti-Phishing Phil , Available: *https://cups.cs.cmu.edu/antiphishing_phil/*

[22] *TrustedSec.* Available: *www.trustedsec.com*

[23] You've heard of phishing – but what is vishing and smishing?:Available: http://www.barfordprimary.co.uk/bham/primary/barford/arenas/websitecontent/web/5.e-safetynewsletterissue5-apr2012.pdf

[24] Anti Phishing phil, Available: http://cups.cs.cmu.edu/ antiphishing_phil/

[25] Anti-phishing,Available: http://www.ucl.ac.uk/cert/antiphishing/

[26] Phishing scam game, Available: https://www.onguard online.gov/media/game-0011-phishing-scams

Author Profile:

Arun Anoop M He obtained his BTech in Computer Science and Engineering from cochin university in the year 2008.He completed his PG diploma in information security and system administration from DOEACC center, NIT , Calicut and obtained his MTech in Information Technology from kalasalingam university in the year 2011. Presently he is a PhD scholar under Anna University,Chennai. He worked as an Assistant Professor in Computer Science and Engineering, MESCE, kuttippuram, kerala. Now he is on study leave for doing his FullTime PhD. Before joining MESCE he worked as teaching assistant in information technology,Kalasalingam university, krishnankoil, Tamilnadu. He is having 3.11 years of teaching experience at MESCE and 6months teaching experience at Kalasalingam University. He has attended many workshops, FDPs and conferences. His areas of interest are network security,WSN,digital forensics,Image Forensics,Multimedia security. He has around 19 conferences and journals. And guided 6 Mtech Main projects.