

Detecting Phishing WebPages

S.S. Kulkarni
Sinhgad Academy of
Engineering, Pune.

Aastha Mittal
Sneha Arondekar
Sinhgad Academy of
Engineering, Pune

Aniket Nayakawadi
Mayank Tomar
Sinhgad Academy of
Engineering, Pune

ABSTRACT

Phishing is basically stealing users personal information (e.g. stealing credit card information or using users banking passwords without any information to the user). Phishing can also be done by making fake web pages as similar as the real, legitimate page and when the user fills information asked in those web pages, they become victim of phishers. There is an urgent need to stop this stealing of information by the Phisher and also for the user to be very careful while filling their personal credentials. User should be sure of the website which they are using, are safe. In the proposed method we are making a website by implementing different APIs which will give user information about the URL and will also be informing user of how safe the particular URL is. We will also be implementing a plug-in through which user will be informed directly about the safety of the URL. If the URL would be safe the plug-in will lead to the page of the plug-in otherwise it will be informing user that the URL is not safe and user should not put their personal information.

Keywords

Anti-phishing, API, website security.

1. INTRODUCTION

Phishing web page imitates the legitimate web page. They are basically used to allure user to put their personal information such as username, passwords or the credit card credentials so that the phishers can use those information for their benefit. Many surveys has been conducted to check how secure the use of internet is but over the years we find more and more phishing sites coming in the market just to grab the details of the user.[3]

As it can be seen from the figure below the number of unique sites that are detected during the year 2014, with this we can say there is an urgent need to stop all this.[1]

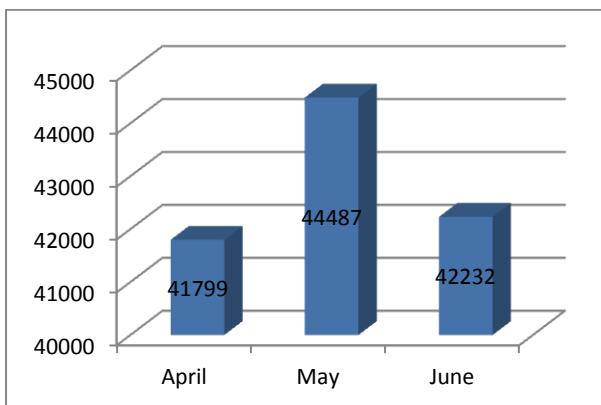


Fig. 1: Unique phishing sites detected April-June 2014

It has been noticed that email users get more spam messages than the normal users and they are the ones who get affected more. As it can be seen from the figure below:[2]

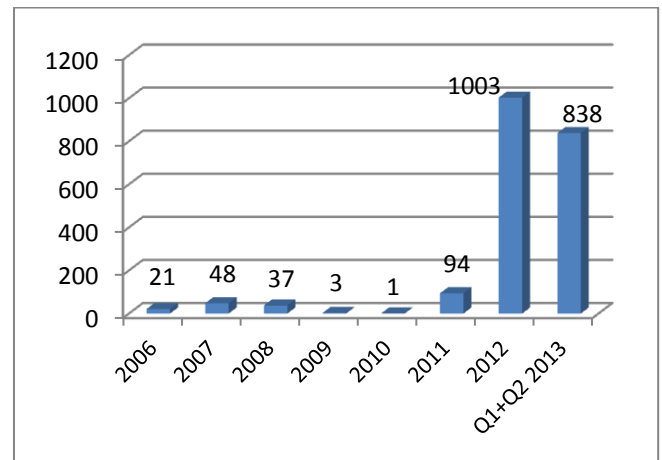


Fig. 2: Number of fraud cases

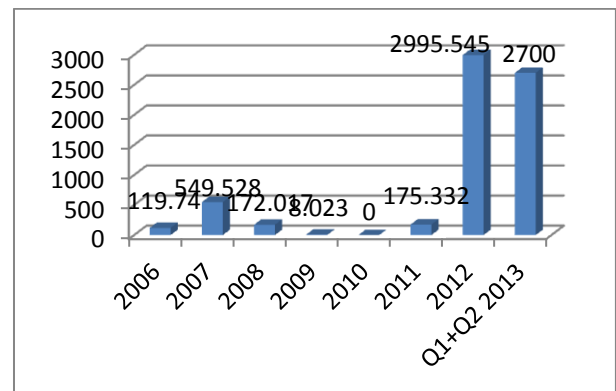


Fig. 3: Loss due to fraud (In EUR)

2. RELATED WORK

If the user is suspicious of the URL received by them in the mails, there can be different ways to check the legitimacy of the URL by the user but before that user should be aware of how to check the URL on their own without using any software.

- A. Firstly the user should check whether the page contains any textbox asking for their credit card number or any finance related personal information, then user should consider it as suspicious and perform step 2.

- B. The user can also check the page by checking how many dots that URL contains. If the URL contains less than 3 dots leaving the “www.” part then it can be considered as legitimate. Otherwise URL should be taken as suspicious.

If the user is still suspicious then he should use the software to check the legitimacy of URL.

3. SYSTEM ARCHITECTURE

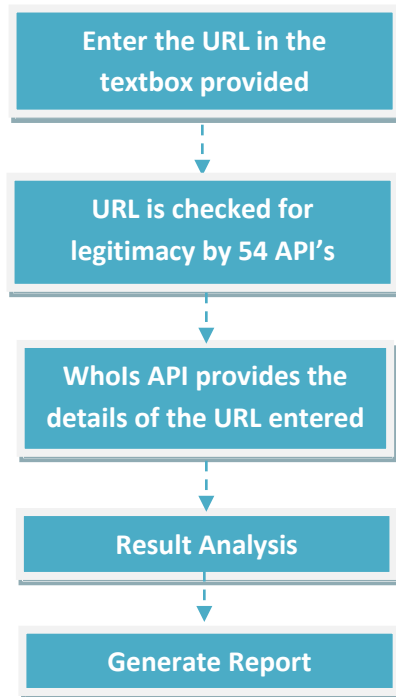


Fig.4: The proposed system architecture

4. SYSTEM DETAILS AND RESULT

- 1) The home page of our website where user enters the URL that he wants check. This is shown in figure below:[7]

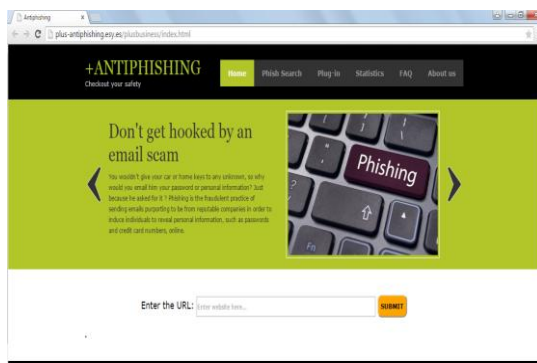


Fig. 5: Homepage of the website.



Fig. 6: Homepage with the URL entered.

- 2) In our project we have implemented 54 API's out of which 1API i.e. WHOIS API gives the detail of the URL entered. The details of the URL are given but some of the details have been extracted which are of some use as it can be seen in the figure below:

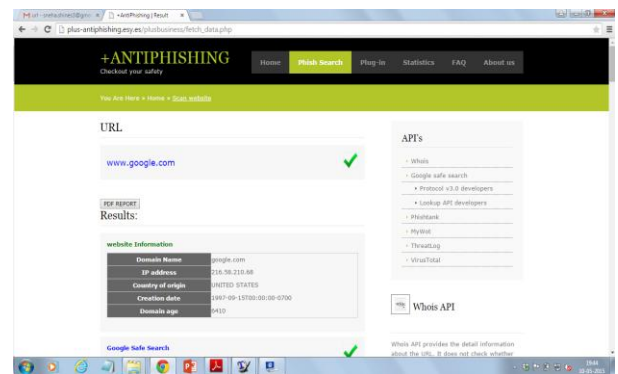


Fig. 7: WHOIS API giving details of the URL entered.

- 3) Depending on the result of the API user is informed about it and also the information about the URL is stored in our database. This is shown below:

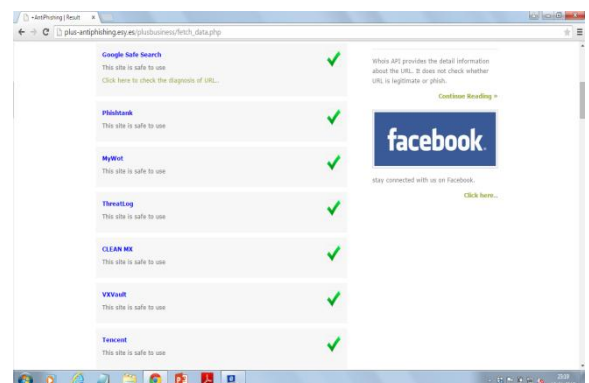


Fig. 8: Different API's Result

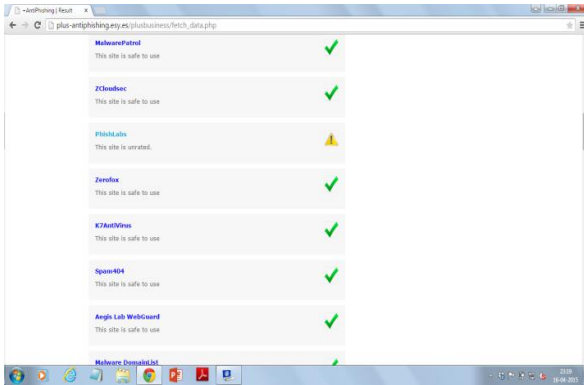


Fig. 9: Positive result of the API for the URL entered.

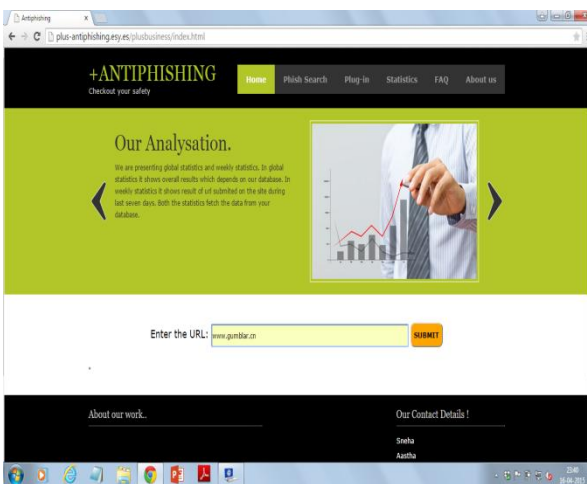


Fig. 10: URL entered to check for legitimacy.

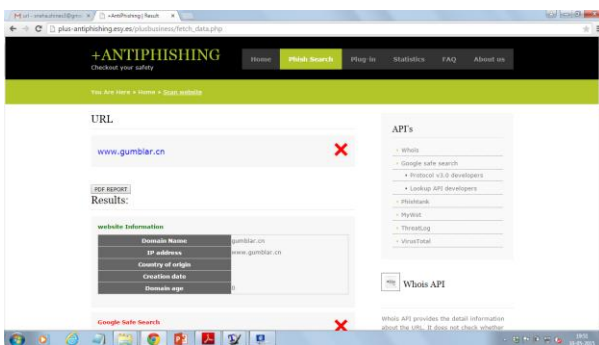


Fig. 11: Detail of the URL entered also it shows the URL is phishy.

Here the green tick means that the particular API is having the data of the URL and also the URL is valid. But as it can be seen there are yellow triangles with the exclamation mark in it, it doesn't mean that the URL is phished. In fact it means that the particular API is not having the data of that particular URL, and the API with the Red Cross means that particular URL is phished according to that API.

- 4) The statistics of the URL checked is also provided and out of those URL checked how many are phished and how many are legal is shown in the figure.

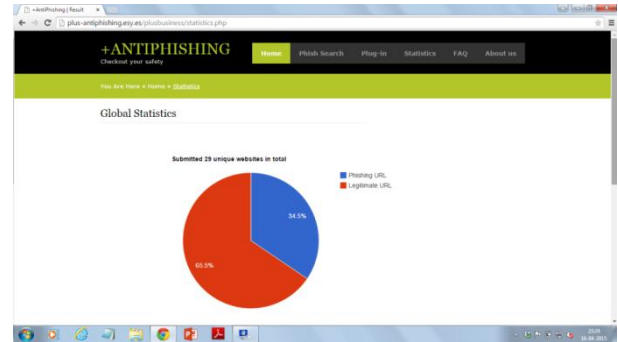


Fig. 12: Statistics to show the legitimacy of different URL's.

- 5) It is also generating pdf report of the URL checked. This can be help the user to check the legitimacy of the url without processing the whole procedure again.



Fig. 13: Report generated for legitimate URL.

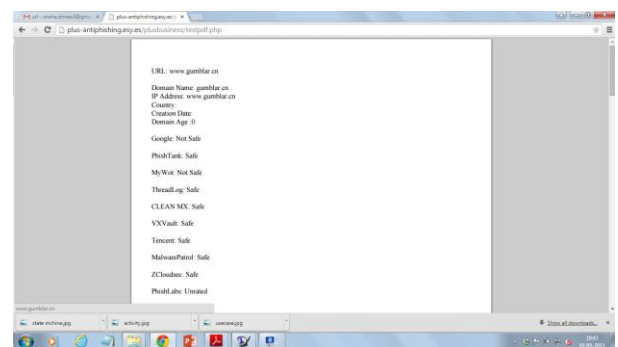
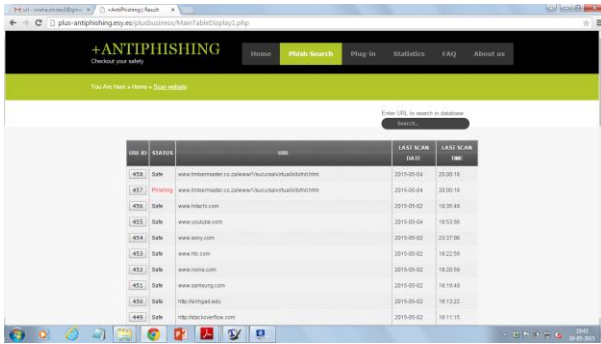


Fig. 14: Report generated for phishy URL.

- 6) Our project is also providing own database so that if the user wishes to check for the url which is recently checked, he can directly view through this database. User can also view the details about the viewed url by clicking on its ID given. This reduces the processing time as user need not to do the whole procedure again. This will also reduce the burden on the database since it will not generate a new ID for the same url checked before.



URL ID	STATUS	URL	LAST SCAN DATE	LAST SCAN TIME
452	Safe	www.internetbanking.be/en/how-prevent-fraud-phishing-never-share-your-personal-internet-banking-data-and-codes	2015-05-04	19:00:18
452	Phishing	www.internetbanking.be/en/how-prevent-fraud-phishing-never-share-your-personal-internet-banking-data-and-codes	2015-05-04	19:00:18
454	Safe	www.youtube.com	2015-05-02	19:30:43
455	Safe	www.youtube.com	2015-05-04	19:33:30
454	Safe	www.etsy.com	2015-05-02	23:37:30
455	Safe	www.etsy.com	2015-05-02	19:22:59
452	Safe	www.mot.com	2015-05-02	19:29:50
455	Safe	www.mot.com	2015-05-02	19:19:43
455	Safe	http://antiphishing.esy.es/plusbusiness/index.html	2015-05-02	19:19:22
445	Safe	http://antiphishing.esy.es/plusbusiness/index.html	2015-05-02	19:11:15

Fig. 15: Database for the URL checked.

5. ADVANTAGES:

- Since 54 API's are implemented in the project, the result can be more efficient and accurate.
- Having our own database to store the details of the URL checked, so if user again tries to check the legitimacy of the same URL the data will be fetched directly from the database, will also reduce the time retrieval of data.
- In the project, the statistics is also provided through which one can get to know how many phished and legitimate URL is registered on the daily basis.

6. CONCLUSION AND FUTURE WORK

By using these API's we have tried to get as efficient result as it should be. With this software user can detect as how many API's agree to the legitimacy of the page and also this would reduce the user to be a victim of the hackers. If any of the API doubts about the legitimacy of the page, user should be careful to put his credentials and this would reduce the crime reports through email.

In near future we can implement more API's so as to make the software as efficient as possible and also to be able to be used by the user blindly.

7. ACKNOWLEDGMENTS

Our thanks to our guide Mr. S.S. Kulkarni who had shown faith in us and also to support us during the making of whole project. We could only complete this project just because of his presence and support.

8. REFERENCES

- [1] How to prevent fraud by phishing: never share your personal internet banking data and codes, Available at: <https://www.safeinternetbanking.be/en/how-prevent-fraud-phishing-never-share-your-personal-internet-banking-data-and-codes>.
- [2] InformationWeek. Available at: <http://www.informationweek.in/informationweek/news-analysis/295570/india-lost-usd-225-million-phishing-attacks-2013-rsa>
- [3] Spam and Phishing, BY DEBORAH FALLOWS. Available at: <http://www.pewinternet.org/2005/04/10/spam-and-phishing>
- [4] About APWG. Available at: <http://www.antiphishing.org/>
- [5] How to prevent fraud by phishing: never share your personal internet banking data and codes. Available at: <https://www.safeinternetbanking.be/en/how-prevent-fraud-phishing-never-share-your-personal-internet-banking-data-and-codes>
- [6] Data Leakage Worldwide: Common Risks and Mistakes Employees Make. Available at: http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.html
- [7] +ANTIPHISHING. Checkout your safety. Available at: <http://plus-antiphishing.esy.es/plusbusiness/index.html>