# Antiphisher

Martina Rodrigues[1], Sneha Gedia[2], Gauri Choudhari[2], Shweta Salekar[2]

[1] *Professor* [2]*Student*

[1] martina.r@xavierengg.com

[2]snehagedia@gmail.com

[2]gaurichoudhari16@gmail.com

[2]shwetasalekar25397@gmail.com

***Abstract*— Social networks have lead to easy and convenient interactions among user irrespective of their geographical location. But at the same time huge amount of sensitive data stored on the Internet possess a constant threat of data being stolen and used in a malicious ways. Phishing is a type of social engineering attack where an attacker tries to steal user sensitive data and use it for a malicious purpose. Phishing attacks are major threat for users carrying out online banking transactions and e-commerce transaction. In this project we have tried to implement a browser extension that will warn users visiting such phishing websites. Antiphisher is implemented as a chrome extension that aims at detecting phishing website URLs based on the URL features identified using machine learning algorithm. Traditional approach for phishing includes blacklisting already known phishing URLs and heuristic based approach. Our approach extends the traditional blacklist method by dynamically extracting URL features that can help in classifying whether the browsed URL is a phishing website or a benign website and thereby alerting user of any malicious activity and preventing intrusion..***

***Keywords*—Phishing, Antiphisher, Machine learning, SVM discriminative classifier, chrome extension**

## I. INTRODUCTION

On one side as Social networking websites have gained most of the popularity for allowing users to interact with each other.[1]People use social networking sites to communicate and share information. Social networking sites makes large sets of data available on the network which threatens user privacy and protection. Phishing is a form of social networking attack in which attacker mimics as a trusted party to lure his victim into malicious schemes. These schemes are sent to the users via SMS, fraud websites, e-mails, etc. Attacker tries to trick user into giving his private information such as Social security number, passwords, credit card number. The attacker later uses such private information for carrying out frauds or for his own benefits. [2]As a traditional information stealing technique, Phishing still works for causing many privacy violation incidents.

Phishing can be defined as -" Phishing is a type of computer attack that communicates socially engineered messages to humans via electronic communication channels in order to persuade them to perform certain actions for the attacker' s benefit."

For example, the attacker persuades the PayPal user to perform certain actions like submitting login credentials to a fake website that looks similar to the official PayPal website.[3]Attacker has to create a visually similar website like PayPal to fool the victim and make him believe it' s an official website. Attacker always tries to target victim into his manipulative scheme that seems attractive to the users, so that attacker can get access to victim' s credentials.

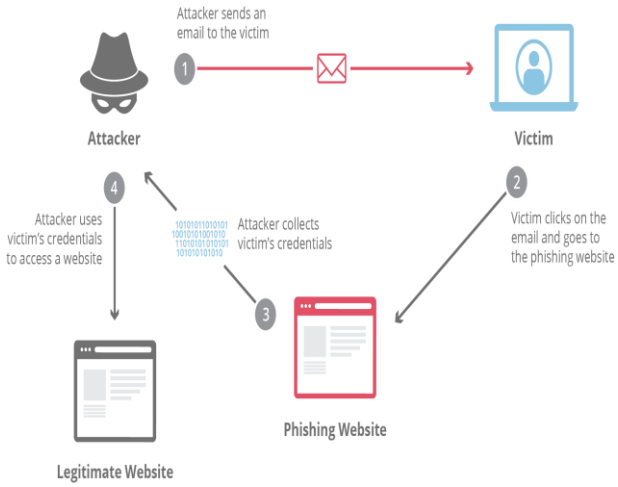


Fig. 1. Phishing attack

The term phishing and its history can be traced back to early 1990s.at that time a group of pirates and hackers formed a community known as ‘ the warez community’ which were considered as the first “ phishers” .[4]Earlier they created an algorithm that allowed them to create an algorithm for generating random credit card numbers. These credit card numbers would be used by hackers to create phony AOL(America Online) accounts. When the phony credit card number is matched with a real card number the attacker were able to create account and spam other users in AOL’ s community by only needing to take a few baits. When AOL was able to stop random credit card generators in year 1995, the warez group had moved onto different methods like accessing as an AOL employee and messaging people via AOL messenger for their information. This quickly became such a problem that on January 2,1996, it was termed as word “ phishing” and was first posted in Usenet group dedicated to AOL. According to Fraud Intelligent Report by the brand protection company MarkMonitor, payment services and financial sector are the most phished industry, accounting for 65.76% of total phishing attacks in quarter three 2012[5].Because of high profitability of these industries there is a rise in number of phishing attacks over the years. In a study by Kaspersky Lab, the number of internet users being attacked worldwide from 2012-2013 has rose to 87%[6].Similarly,Anti-phishing Working Group(APWG) has recorded a number of 45,628 unique phishing websites in December 2012[7], as compared to 26,124 in December 2010[8].To protect Internet users from being phished, we propose a phishing detection approach that determines whether the browsed URL is phishing or legitimate and allows the user to blacklist the URLs that are found to be phishing. It target various URL features of phishing websites that are learned using machine learning algorithms on ‘ Phishing Website Dataset’ from UCI Machine Learning Repository. Antiphisher is implemented as a chrome extension which will then check whether the targeted features are present in the URL submitted by the user and if the URL is added in the list of blacklist URLs. If any above is true then the user would be alarmed about the same.

## II. RELATED WORK

### *A. Blacklist/Whitelist based approach*

This method of detection is most widely used in browsers such as Google Chrome and Mozilla Firefox for safe browsing. [2]Depending on the method of implementation either the user maintains a list of whitelist and blacklist URLs or the browser automatically updates the lists. The blacklisted URLs contains the list of websites that are found malicious by the browser. [2]Classifiers such as Naive Bayesian, SVM etc. are used to maintain the whitelist of the websites that safe for user browsing. Although easy to implement it faces the issue of high false negative ratio due to short lifetime of phishing web pages. The main drawback of this approach is that they are not effective on the web pages which were previously undetected and hence the lists needs to be maintained frequently to have a good accuracy.

### *B. URL based detection*

URL based approach analyse the URL features of the given web pages and based on this features a decision is made whether the website is phishing or not. [3]URL features such as length, path, hostname, no. of tokens present are different for a legitimate and a phishing website. This property is exploited in this approach. Lexical analysis is performed on the URL in order to extract URL features. To maintain and update the feature list of URL properties, a classifier is employed that can successfully distinguish between the features of actual website and a malicious website and thereby can make an appropriate decision for the suspicious webpage’ s URL.

### *C. Content-based detection*

In content based detection, the [2]visual similarity between a malicious page and target page is the key feature to detect phishing attacks. The visual features considered can be text and styles, images and the overall appearance of the web pages. The [10] study proposes an algorithm that detects the phishing pages on basis of contents of the web-page, using term frequency - inverse document frequency(TF-IDF). This cannot be resilient to evasion as the attacker can change the contents and still may make feel the website as the original one to user. So to deal with this some approaches to [2]detect phishing consider capturing image of the page and convert it into text using optical character recognition(OCR) and uses the Google PageRank algorithm to find the top rank domains from search engines and compares them with the current page. Another study [2] considers the textual clues from the DOM tree of the website to detect any anomalies in the DOM Objects. A file similarity is calculated between the targeted file and the suspicious web page so as to easily find out potential phishing web pages effectively.

### *D. Phishing detection based on other features*

Other features such as domain owner differs of an actual website and the fake website. As the phishing web pages are hosted on a less reputable domain and are usually taken down more frequently, this property can be used to decide whether the webpage given is phishing or not. A [10]WHOIS Lookup is conducted to reveal the registrar given webpage and the registrar of the legitimate webpage .This is found using search engine analysis tools. Then these both domain owners are checked if the registrars for the suspicious and the legitimate website does not match then it is declared as phishing website.

## III. Proposed Approach

Other features such as domain owner differs of an actual website and the fake website. As the phishing web pages are hosted on a less reputable domain and are usually taken down more frequently, this property can be used to decide whether the webpage given is phishing or not. A [10]WHOIS Lookup is conducted to reveal the registrar given webpage and the registrar of the legitimate webpage .This is found using search engine analysis tools. Then these both domain owners are checked if the registrars for the suspicious and the legitimate website does not match then it is declared as phishing website.

## IV. Proposed Approach

The proposed system will use machine learning algorithms like SVM(Support Vector Machine),Random Forest, Artificial Neural Network on the phishing website dataset for generating a model to classify website as phishing or not phishing. The SVM algorithm giving learned model with the highest accuracy ,less computational time and low false positive and false negative ratio is used for deploying a chrome extension which can be used to detect phishing websites. This chrome extension will then check the URL features learned from the selected model to predict whether a given page is phishing page or a benign one and alarm the user if it predicts a page to be illegitimate.

## V. Dataset

The proposed system will be using machine learning algorithms to classify the [9]dataset ‘ Phishing Websites Dataset’ from UCI Machine learning repository. The dataset consists of 11,055 entries with 6157 phishing instances and 4898 legitimate instances. Each instance consists of 30 features comprising of various attributes typically associated with phishing or suspicious web pages such as presence of IP address in the URL domain or presence of JavaScript code to modify the web browser address bar information. Each feature is associated with a rule. If the rule is satisfied, we take it as an indicator of phishing and benign otherwise. The [9]dataset has been normalized to contain only discrete values. Each feature of each instance will contain ’ 1’ if the rule associated with that feature is satisfied, ’ 0’ if partially satisfied and ’ -1’ if unsatisfied.

## VI. Machine Learning Implementation

Machine learning implementation trains and tests the data to classify the dataset mentioned into phishing and not phishing based on its URL properties present in the URL using three algorithms Random Forest, Artificial neural network, Support Vector Machine(SVM). The dataset was split into training and test set in the ratio 7:3.The evaluation of the various classifying algorithm is done using Python programming. Two input data files Dataset.csv and Target_labels.csv are given to the program. In our experiment .csv file format was used. The program run the Dataset and Target_labels files to calculate True Positive(TP),False Positive(FP),True Negative(TN),False Negative(FN) rates, Sensitivity, Specificity and running time for an algorithm:

The three machine learning algorithms considered for processing the feature set are:

### *A. Random Forest:*

A random forest is a data construct applied to machine learning that develops large numbers of random [14] decision trees analysing sets of variables. This type of algorithm helps to enhance the ways that technologies analyse complex data. One way to describe the philosophy behind the random forest is that since the random trees have some overlap, engineers can build systems to study data redundantly with the various trees and look for trends and patterns that support a given data outcome.

### *B. Artificial neural network:*

An artificial neuron network (ANN) is a [14]computational model based on the structure and functions of biological neural networks. Information that flows through the network affects the structure of the ANN because a neural network changes - or learns, in a sense - based on that input and output. ANNs are considered nonlinear statistical data modeling tools where the complex relationships between inputs and outputs are modeled or patterns are found. ANNs have three layers that are interconnected. The first layer consists of input neurons. Those neurons send data on to the second layer, which in turn sends the output neurons to the third layer.

### *C. SVM (Support Vector Machine):*

The SVM performs classification by finding [1] the hyperplane that maximizes the margin between two classes. The vectors that define the hyperplane are the support vectors.

The results obtained from all the above three algorithms is been discussed in the ML analysis section.

## VII. Machine Learning Analysis

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

This project compares the performance of all the classifiers described in section 6 on the phishing dataset. We have evaluated these algorithms on 3317 test samples using various performance metrics and this section contains the tabulated results.

| | Predicted Phishing URLs | Predicted Legitimate URLs |
|---|---|---|
| Ground Truth Phishing URLs | 1249 | 162 |
| Ground Truth Legitimate URLs | 182 | 1680 |

Fig. 2. TABLE I: Random forest Confusion Matrix

Table I (Fig. 2.) shows the confusion matrix for Random forests. With 1249 true positives, 182 false positives, 162 false negatives and 1680 true negatives.

| | Predicted Phishing URLs | Predicted Legitimate URLs |
|---|---|---|
| Ground Truth Phishing URLs | 1205 | 250 |
| Ground Truth Legitimate URLs | 170 | 1692 |

Fig. 3. TABLE II: Artificial Neural Network Confusion Matrix

Table II (Fig. 3.) shows the confusion matrix for artificial neural network. With 1205 true positives, 170 false positives, 250 false negatives and 1692 true negatives.

| | Predicted Phishing URLs | Predicted Legitimate URLs |
|---|---|---|
| Ground Truth Phishing URLs | 1293 | 206 |
| Ground Truth Legitimate URLs | 131 | 1731 |

Fig. 4. TABLE III: SVM Confusion Matrix

Table III (Fig. 4.) shows the confusion matrix for Support vector machine. With 1293 true positives, 206 false positives, 131 false negatives and 1731 true negatives.

| | Accuracy(%) | Specificity(%) | Sensitivity(%) |
|---|---|---|---|
| Artificial Neural Network | 87.34 | 91 | 83 |
| Random Forest | 89.63 | 90 | 86 |
| SVM | 89.84 | 93 | 89 |

Fig. 5. TABLE IV: Performance matrix of classifiers

In Table IV (Fig. 5.), sensitivity refers to the classifier' s ability to correctly detect phishing URLs. It can be seen that SVM has the highest sensitivity among all the other classifiers. However, in phishing detection, false positives and false negatives are given more consideration when studying the performance (predictive accuracy) of a classifier. That is because false positives are more expensive than false negatives in the real world. Since we do not want to allow users to access the phishing URLs, false positives are considered to be important while deciding the best classifier.

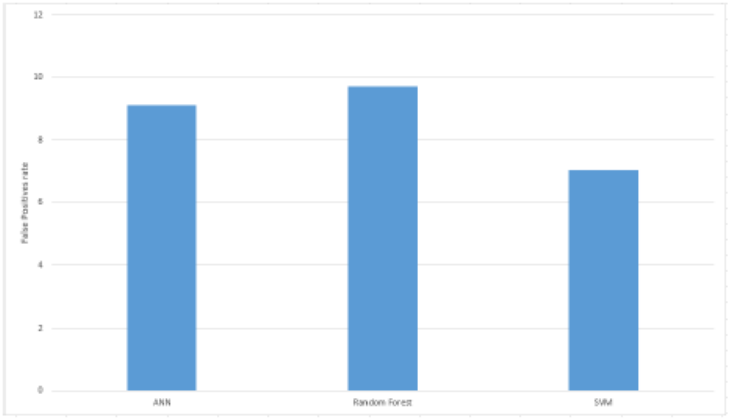


Fig. 6. False positive rate of classifiers

The Table 4 and the above graph (Fig. 6.) of false positive rates shows the performance of all the classifiers. It is evident that SVM has the highest accuracy, specificity and sensitivity among the three along with the least false positive rate. Hence, SVM works best in classifying the phishing URL from the legitimate URLs.

## VIII. EXTENSION IMPLEMENTATION

The proposed approach aims at building a browser extension powered by machine learning technique for phishing detection. The SVM algorithm giving learned model with the highest accuracy, less computational time and low false positive and false negative ratio is used for deploying a chrome extension, which can be used to detect phishing websites. The extension is packaged to support Chrome browser in specific, solely by the virtue of its popularity. Additionally, extensions exhibit minimal web-dependence, as it collates multiple files into single file for user to download, as one-time activity.

The persistent model based SVM discriminative classifier trained using available dataset is used by the extension to predict the authenticity of the user accessed web page and alert user the legitimacy of the web page. This solution integrates a python based training implementation and a JavaScript based testing module.

The chrome extension compiles to the google norms and primarily consists of three main files: manifest.json, background.js, content.js. The metadata about the chrome extension is given in the manifest file. The content.js runs with loading of every page and has access to the DOM elements. It uses supporting files to interact with external APIs and browser user interface manipulation. The background.js performs message passing to aid these type of interactions.

The content.js script has multiple functions that perform web content and URL feature extraction. Below are some of the details of features used to identify illegitimate webpages:

isIPInURL(): Identify presence of IP address in the URL

isLongURL(): Validate if length of the URL is beyond 75 characters

isTinyURL(): Identify URLs smaller than 20 charaters

isAlphaNumericURL(): Check for alphanumeric ’ @’ in URL

isRedirectingURL(): Verify if ’ //’ existing within the URL more than once

isHypenURL(): Check for presence of ’ -’ adjacent to domain name in URL

isMultiDomainURL(): Domain name should be confined to top-level domain, country-code and second-level domain.

isFaviconDomainUnidentical(): Verify if links on given webpage are loaded from other domains

isIllegalHttpsURL(): Identify presence of multiple ’ https’ in the URL string

isImgFromDifferentDomain(): Validate if images on given web-page are loaded from other domains

isAnchorFromDifferentDomain(): Detect if links on given web-page are loaded from other domains

isScLnkFromDifferentDomain(): Identify if scripts on given web-page are loaded from other domains

isFormActionInvalid(): Detect invalid/blank form submissions

isMailToAvailable(): Check for anchor tag incorporating mailto

isStatusBarTampered(): Validate if onmouseover manipulates the status bar display

isIframePresent(): Identify sites, which exhibit iframes in the DOM

These features are passed through the persistent model to predict the authenticity of the webpage.

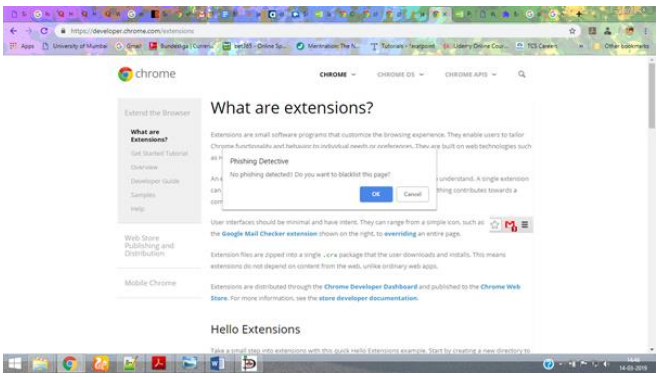


Fig. 7. Antiphisher Alert-1

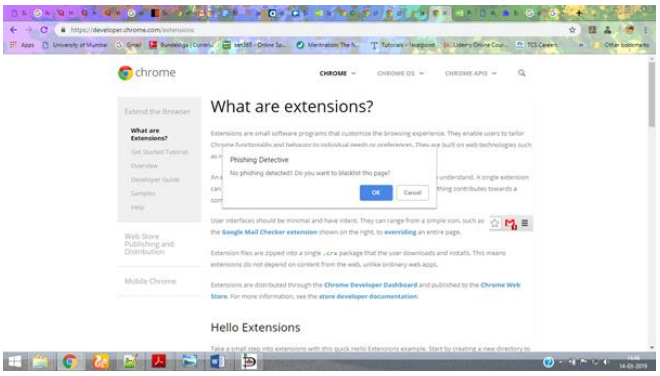


Fig. 8. Antiphisher Alert-2

The above images (Fig. 7. and Fig. 8.) are the output given by our chrome extensions, which gives the decision whether the browsed URL is Phishing detected or no phishing detected and if the URL is Phishing it will allow user to mark that URL as blacklisted URL.

## IX. CONCLUSION

We have seen how major problem phishing can be and its continuously changing patterns, which makes it difficult to detect new trends. we will experiment with three machine learning algorithms on a dataset of features that represent attributes commonly associated with phishing pages, choose the best model based on their performance and build a web browser plugin. To protect users from visiting fake websites, we tried to identify phishing URLs based on the features extracted. A particular challenge in this domain is that user is constantly making new strategies to counter our defence. The users are also provided to make their blacklist for future reference. The extension allows easy deployment of our phishing detection model to end users. For future enhancements, we intend to build the phishing detection system as a scalable web service which will incorporate online learning so that new phishing attack patterns can easily be learned and improve the accuracy of our models with better feature extraction.

## REFERENCES

[1] Joby James,Sandhya L.,Ciza Thomas“ Detection of phishing URL using machine learning techniques”
[2] Phishing-Alarm: Robust and Efficient Phishing Detection via Page Component Similarity JIAN MAO, (Member, IEEE), WENQIAN TIAN, PEI LI, TAO WEI, (Member,IEEE), AND ZHENKAI LIANG, (Member, IEEE).
[3] Phishing Detection: A Literature Survey Mahmoud Khonji, Youssef Iraqi, Senior Member, IEEE, and Andrew Jones.
[4] https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-definition-and-history/#gref
[5] (2014, June) Fraud intelligence report - third quarter 2012.MarkMonitor Inc. [Online]. Available: https://www.markmonitor.com/download/report/Fraud Report-Q3 2012.pdf
[6] (2014, June) The evolution of phishing attacks:2011-2013. Kaspersky Lab ZAO. [Online]. Available:http://media.kaspersky.com/pdf/Kaspersky Lab KSN report The Evolution of Phishing Attacks 2011-2013.pdf
[7] (2014, June) Phishing activity trends report, 4th quarter 2012.Anti-Phishing Working Group. [Online]. Available: http://docs.apwg.

[8] (2014, June) Phishing activity trends report, 2nd half / 2010.Anti-Phishing Working Group. [Online]. Available: http://docs.apwg.org/reports/apwg report h2 2010.pdf
[9] " Machine Learning Approach to Phishing Detection " Arvind Rekha Sura,Jyoti Kini,Kishan Athrey
[10] " Phishing Website Detection Using URL-Assisted Brand Name Weighting System" Choon Lin Tan, Kang Leng Chiewy, San Nah Szez
[11] (2014, June) Digicert phishing white paper: A primer on what phishing is and how it works. DigiCert, Inc. [Online]. Available:http://www.digicert.com/news/DigiCert Phishing White Paper.pdf
[12] (2014, June) Fraud alert: New phishing tactics - and how they impact your business.Thawte,Inc.[Online].Available:https://community.thawte.com/system/files/download-attachments/Phishing%20WP D2.pdf
[13] (2014, June) Rsa monthly online fraud report – january 2014. EMC Corporation. [Online]. Available: http://www.emc.com/collateral/fraudreport/rsa-online-fraud-report-012014.pdf
[14] https://www.techopedia.com