Phishing Website Detection

*PROJECT REPORT*

*Submitted in the partial fulfilment of the requirements for award of the*

**Six Months Online Certificate Course**

*in*

**Cyber Security**

**Course Duration: [22-01-2024 to 21-07-2024]**

By

 Ravikiran Dushetti

 (HT.No.2406CYS119)

Under the Esteemed Guidance

Prof P. Penchalaiah



# DIRECTORATE OF INNOVATIVE LEARNING & TEACHING (DILT)

## JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

(Formerly SCDE\_SCHOOL OF CONTINUING AND DISTANCE EDUCATION)

Kukatpally, Hyderabad, Telangana State, INDIA- 500 085

**JULY 2024**

# ABSTRACT

Phishing attacks are a type of social engineering attack where criminals use fraudulent emails, text messages, or websites to trick victims into revealing sensitive information such as passwords, credit card numbers, or bank account details.

Phishing attacks pose a significant threat to internet users, leading to substantial financial losses and compromised personal information. This project aims to develop an effective phishing website detection system using machine learning techniques. By analyzing various features such as URL characteristics, website content, and metadata, the system can accurately distinguish between legitimate and phishing websites. The proposed solution leverages a combination of supervised learning algorithms and feature extraction methods to enhance detection accuracy. Experimental results demonstrate the system’s robustness and efficiency in identifying phishing websites, thereby providing a valuable tool for enhancing cybersecurity and protecting users from online fraud.

***Keywords****:* cybersecurity, phishing, python, Machine Learning.

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **Chapter No** | **Chapter Name** | **Page Number** |
| 1. | Introduction | 4 |
| 2. | Literature Survey | 5 |
| 3. | Problem Statement | 6 |
| 4. | Objectives | 9 |
| 5. | Methodology | 10 |
| 6. | Algorithms | 13 |
| 7. | Results & Analysis | 14 |
| 8. | Conclusion | 17 |
| 9. | Future Scope | 17 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**INTRODUCTION**

Cyber security is the technology and process that is designed to protect networks and devices, data from attack, damage, or unauthorized access.

As most of the tasks digitalized and data is exposed to internet which puts people at risk such as phishing, scams, spam and leak of PII and compromising their privacy.

These examples represent only a fraction of the various cyber-attacks. Maintaining vigilance and implementing suitable measures is crucial to safeguard yourself and your devices against such threats



**Phishing**:

Phishing attacks are a type of social engineering attack where criminals use fraudulent emails, text messages, or websites to trick victims into revealing sensitive information such as passwords, credit card numbers, or bank account details.

**How does Phishing work?**

Anyone who uses the internet or phones can be a target for phishing scammers.

Phishing scams normally try to:

* + Infect your device with malware
	+ Steal your private credentials to get your money or identity
	+ Obtain control of your online accounts
	+ Convince you to willingly send money or valuables

Sometimes these threats don’t stop with you. If a hacker gets into your email, contact list, or social media, they can spam people you know with phishing messages seemingly from you.



# Literature Survey

Phishing is a form of fraudulent attack where the attacker tries to gain sensitive information by posing as a reputable source. In a typical phishing attack, a victim opens a compromised link that poses as a credible website. The victim is then asked to enter their credentials, but since it is a “fake” website, the sensitive information is routed to the hacker and the victim gets ”‘hacked.”

Phishing is popular since it is a low effort, high reward attack. Most modern web browsers, antivirus software and email clients are pretty good at detecting phishing websites at the source, helping to prevent attacks. To understand how they work, this blog post will walk you through a tutorial that shows you how to build your own phishing URL detector using Python and machine learning:

1. **Identify the criteria** that can recognize fake URLs
2. **Build a decision tree** that can iterate through the criteria
3. **Train our model** to recognize fake vs real URLs
4. **Evaluate our model** to see how it performs
5. **Check for false positives/negatives**



# Objectives

A phishing website is a common social engineering method that mimics trustful uniform resource locators (URLs) and webpages. The objective of this project is to train machine learning models and deep neural nets on the dataset created to predict phishing websites. Both phishing and benign URLs of websites are gathered to form a dataset and from them required URL and website content-based features are extracted. The performance level of each model is measured and compared.

Phishing attacks are categorized according to Phisher’s mechanism for trapping alleged users. Several forms of these attacks are keyloggers, DNS toxicity, Etc., The initiation processes in social engineering include online blogs, short message services (SMS), social media platforms that use web 2.0 services, such as Facebook and Twitter, file-sharing services for peers, Voice over IP (VoIP) systems where the attackers use caller spoofing IDs. Each form of phishing has a little difference in how the process is carried out to defraud the unsuspecting consumer. E-mail phishing attacks occur when an attacker sends an e-mail with a link to potential users to direct them to phishing websites.



# Methodology

In my project, I will study the important features of websites and create a dataset to predict and forecast phishing attacks.

Here are the key features I am going to feed in comparative model:

**1. Address Bar based Features**

## Using the IP Address

If an IP address is used as an alternative of the domain name in the URL, such as “<http://125.98.3.123/fake.html>”, users can be sure that someone is trying to steal their personal information. Sometimes, the IP address is even transformed into hexadecimal code as shown in the following link “[http://0x58.0xCC.0xCA.0x62/2/paypal.ca/index.html](http://88.204.202.98/2/paypal.ca/index.html)”.

Rule is: If The Domain Part has an IP Address → Phishing

{ Otherwise → Legitimate

## Long URL to Hide the Suspicious Part

Phishers can use long URL to hide the doubtful part in the address bar. For example:

[http://federmacedoadv.com.br/3f/aze/ab51e2e319e51502f416dbe46b773a5e/?cmd=\_home&amp;disp](http://federmacedoadv.com.br/3f/aze/ab51e2e319e51502f416dbe46b773a5e/?cmd=_home&amp%3Bdispatch=11004d58f5b74f8dc1e7c2e8dd4105e811004d58f5b74f8dc1e7c2e8dd4105e8) [atch=11004d58f5b74f8dc1e7c2e8dd4105e811004d58f5b74f8dc1e7c2e8dd4105e8](http://federmacedoadv.com.br/3f/aze/ab51e2e319e51502f416dbe46b773a5e/?cmd=_home&amp%3Bdispatch=11004d58f5b74f8dc1e7c2e8dd4105e811004d58f5b74f8dc1e7c2e8dd4105e8)@phishing.website. html

To ensure accuracy of our study, we calculated the length of URLs in the dataset and produced an average URL length. The results showed that if the length of the URL is greater than or equal 54 characters then the URL classified as phishing. By reviewing our dataset we were able to find 1220 URLs lengths equals to 54 or more which constitute 48.8% of the total dataset size.

𝑈𝑅𝐿 𝑙𝑒𝑛𝑔𝑡ℎ < 54 → 𝑓𝑒𝑎𝑡𝑢𝑟𝑒 = Legitimate

*Rule: IF*{ 𝑒𝑙𝑠𝑒 𝑖𝑓 𝑈𝑅𝐿 𝑙𝑒𝑛𝑔𝑡ℎ ≥ 54 𝑎𝑛𝑑 ≤ 75 → 𝑓𝑒𝑎𝑡𝑢𝑟𝑒 = 𝑆𝑢𝑠𝑝𝑖𝑐𝑖𝑜𝑢𝑠

𝑜𝑡ℎ𝑒𝑟𝑤𝑖𝑠𝑒 → 𝑓𝑒𝑎𝑡𝑢𝑟𝑒 = Phishing

We have been able to update this feature rule by using a method based on frequency and thus improving upon its accuracy.

## Using URL Shortening Services “TinyURL”

URL shortening is a method on the “World Wide Web” in which a URL may be made considerably smaller in length and still lead to the required webpage. This is accomplished by means of an “HTTP Redirect” on a domain name that is short, which links to the webpage that has a long URL. For example, the URL [“http://portal.hud.ac.uk/](http://portal.hud.ac.uk/)” can be shortened to “bit.ly/19DXSk4”.

*Rule*: IF{ TinyURL → Phishing Otherwise → Legitimate

## URL’s having “@” Symbol

Using “@” symbol in the URL leads the browser to ignore everything preceding the “@” symbol and the real address often follows the “@” symbol.

Rule: IF Url Having @ Symbol → Phishing

 { Otherwise → Legitimate

## Redirecting using “//”

The existence of “//” within the URL path means that the user will be redirected to another website. An example of such URL’s is: “http://www.legitimate.com//[http://www.phishing.com](http://www.phishing.com/)”. We examin the location where the “//” appears. We find that if the URL starts with “HTTP”, that means the “//” should appear in the sixth position. However, if the URL employs “HTTPS” then the “//” should appear in seventh position.

Rule: IF ThePosition of the Last Occurrence of "//" in the URL > 7 → Phishing

 { Otherwise → Legitimate

## Adding Prefix or Suffix Separated by (-) to the Domain

The dash symbol is rarely used in legitimate URLs. Phishers tend to add prefixes or suffixes separated by (-) to the domain name so that users feel that they are dealing with a legitimate webpage. For example [http://www.Confirme-paypal.com/.](http://www.Confirme-paypal.com/)

Rule: IF Domain Name Part Includes (−) Symbol → Phishing

 { Otherwise → Legitimate

## Sub Domain and Multi Sub Domains

Let us assume we have the following link: [http://www.hud.ac.uk/students/.](http://www.hud.ac.uk/students/) A domain name might include the country-code top-level domains (ccTLD), which in our example is “uk”. The “ac” part is shorthand for “academic”, the combined “ac.uk” is called a second-level domain (SLD) and “hud” is the actual name of the domain. To produce a rule for extracting this feature, we firstly have to omit the (www.) from the URL which is in fact a sub domain in itself. Then, we have to remove the (ccTLD) if it exists. Finally, we count the remaining dots. If the number of dots is greater than one, then the URL is classified as “Suspicious” since it has one sub domain. However, if the dots are greater than two, it is classified as “Phishing” since it will have multiple sub domains. Otherwise, if the URL has no sub domains, we will assign “Legitimate” to the feature.

Dots In Domain Part = 1 → Legitimate

Rule: IF {Dots In Domain Part = 2 → Suspicious

Otherwise → Phishing

## HTTPS (Hyper Text Transfer Protocol with Secure Sockets Layer)

The existence of HTTPS is very important in giving the impression of website legitimacy, but this is clearly not enough. The authors in (Mohammad, Thabtah and McCluskey 2012) (Mohammad, Thabtah and McCluskey 2013) suggest checking the certificate assigned with HTTPS including the extent of the trust certificate issuer, and the certificate age. Certificate Authorities that are consistently listed among the top trustworthy names include: “GeoTrust, [GoDaddy,](http://www.godaddy.com/gdshop/ssl/ssl.asp?isc=BESTSSL1) Network Solutions, Thawte, Comodo, Doster and VeriSign”. Furthermore, by testing out our datasets, we find that the minimum age of a reputable certificate is two years.

Use https and Issuer Is Trusted and Age of Certificate ≥ 1 Years → Legitimate

Rule: IF{

Using https and Issuer Is Not Trusted → Suspicious Otherwise → Phishing

## Domain Registration Length

Based on the fact that a phishing website lives for a short period of time, we believe that trustworthy domains are regularly paid for several years in advance. In our dataset, we find that the longest fraudulent domains have been used for one year only.

Rule: IF{Domains Expires on ≤ 1 years → Phishing

Otherwise → Legitimate

## Favicon

A favicon is a graphic image (icon) associated with a specific webpage. Many existing user agents such as graphical browsers and newsreaders show favicon as a visual reminder of the website identity in the address bar. If the favicon is loaded from a domain other than that shown in the address bar, then the webpage is likely to be considered a Phishing attempt.

Rule: IF{Favicon Loaded From External Domain → Phishing

Otherwise → Legitimate

## Using Non-Standard Port

This feature is useful in validating if a particular service (e.g. HTTP) is up or down on a specific server. In the aim of controlling intrusions, it is much better to merely open ports that you need. Several firewalls, Proxy and Network Address Translation (NAT) servers will, by default, block all or most of the ports and only open the ones selected. If all ports are open, phishers can run almost any service they want and as a result, user information is threatened. The most important ports and their preferred status are shown in Table 2.

Rule: IF{Port # is of the Preffered Status → Phishing

Otherwise → Legitimate

**Table 1 Common ports to be checked**

|  |  |  |  |
| --- | --- | --- | --- |
| PORT | Service | Meaning | Preferred Status |
| 21 | FTP | Transfer files from one host to another | Close |
| 22 | SSH | Secure File Transfer Protocol | Close |
| 23 | Telnet | provide a bidirectional interactive text-oriented communication | Close |
| 80 | HTTP | Hyper test transfer protocol | Open |
| 443 | HTTPS | Hypertext transfer protocol secured | Open |
| 445 | SMB | Providing shared access to files, printers, serial ports | Close |
| 1433 | MSSQL | Store and retrieve data as requested by other software applications | Close |
| 1521 | ORACLE | Access oracle database from web. | Close |
| 3306 | MySQL | Access MySQL database from web. | Close |
| 3389 | Remote Desktop | allow remote access and remote collaboration | Close |

## The Existence of “HTTPS” Token in the Domain Part of the URL

The phishers may add the “HTTPS” token to the domain part of a URL in order to trick users. For example,

[http://https-www-paypal-it-webapps-mpp-home.soft-hair.com/.](http://https-www-paypal-it-webapps-mpp-home.soft-hair.com/)

Rule: IF{Using HTTP Token in Domain Part of The URL → Phishing

Otherwise → Legitimate

# Abnormal Based Features

## Request URL

Request URL examines whether the external objects contained within a webpage such as images, videos and sounds are loaded from another domain. In legitimate webpages, the webpage address and most of objects embedded within the webpage are sharing the same domain.

% of Request URL < 22% → Legitimate

Rule: IF {%of Request URL ≥ 22% and 61% → Suspicious Otherwise → feature = Phishing

## URL of Anchor

An anchor is an element defined by the <a> tag. This feature is treated exactly as “Request URL”. However, for this feature we examine:

1. If the <a> tags and the website have different domain names. This is similar to request URL feature.
2. If the anchor does not link to any webpage, e.g.:
	1. <a href=“#”>
	2. <a href=“#content”>
	3. <a href=“#skip”>
	4. <a href=“JavaScript ::void(0)”>

% of URL Of Anchor < 31% → 𝐿𝑒𝑔𝑖𝑡𝑖𝑚𝑎𝑡𝑒

*Rule*: IF{% of URL Of Anchor ≥ 31% And ≤ 67% → Suspicious

Otherwise → Phishing

## Links in <Meta>, <Script> and <Link> tags

Given that our investigation covers all angles likely to be used in the webpage source code, we find that it is common for legitimate websites to use <Meta> tags to offer metadata about the HTML document; <Script> tags to create a client side script; and <Link> tags to retrieve other web resources. It is expected that these tags are linked to the same domain of the webpage.

Rule:

% of Links in " < Meta > ", " < Script > " and " < Link>" < 17% → Legitimate

IF{% of Links in < Meta > ", " < Script > " and " < Link>" ≥ 17% And ≤ 81% → Suspicious

Otherwise → Phishing

## Server Form Handler (SFH)

SFHs that contain an empty string or “about:blank” are considered doubtful because an action should be taken upon the submitted information. In addition, if the domain name in SFHs is different from the domain name of the webpage, this reveals that the webpage is suspicious because the submitted information is rarely handled by external domains.

SFH is "about: blank" Or Is Empty → Phishing

Rule: IF{ SFH Refers To A Different Domain → Suspicious

Otherwise → Legitimate

## Submitting Information to Email

Web form allows a user to submit his personal information that is directed to a server for processing. A phisher might redirect the user’s information to his personal email. To that end, a server-side script language might be used such as “mail()” function in PHP. One more client-side function that might be used for this purpose is the “mailto:” function.

Rule: IF{Using "mail()" or "mailto:" Function to Submit User Information → Phishing

Otherwise → Legitimate

## Abnormal URL

This feature can be extracted from WHOIS database. For a legitimate website, identity is typically part of its URL.

Rule: IF

The Host Name Is Not Included In URL → Phishing

{ Otherwise → Legitimate

# HTML and JavaScript based Features

## Website Forwarding

The fine line that distinguishes phishing websites from legitimate ones is how many times a website has been redirected. In our dataset, we find that legitimate websites have been redirected one time max. On the other hand, phishing websites containing this feature have been redirected at least 4 times.

#ofRedirect Page ≤ 1 → Legitimate

Rule: IF {#of Redirect Page ≥ 2 And < 4 → Suspicious

Otherwise → Phishing

## Status Bar Customization

Phishers may use JavaScript to show a fake URL in the status bar to users. To extract this feature, we must dig-out the webpage source code, particularly the “onMouseOver” event, and check if it makes any changes on the status bar.

Rule: IF{onMouseOver Changes Status Bar → Phishing It Does′t Change Status Bar → Legitimate

## Disabling Right Click

Phishers use JavaScript to disable the right-click function, so that users cannot view and save the webpage source code. This feature is treated exactly as “Using onMouseOver to hide the Link”. Nonetheless, for this feature, we will search for event “event.button==2” in the webpage source code and check if the right click is disabled.

Rule: IF{Right Click Disabled → Phishing

Otherwise → Legitimate

## Using Pop-up Window

It is unusual to find a legitimate website asking users to submit their personal information through a pop-up window. On the other hand, this feature has been used in some legitimate websites and its main goal is to warn users about fraudulent activities or broadcast a welcome announcement, though no personal information was asked to be filled in through these pop-up windows.

Rule: IF

Popoup Window Contains Text Fields → Phishing

{ Otherwise → Legitimate

## IFrame Redirection

IFrame is an HTML tag used to display an additional webpage into one that is currently shown. Phishers can make use of the “iframe” tag and make it invisible i.e. without frame borders. In this regard, phishers make use of the “frameBorder” attribute which causes the browser to render a visual delineation.

Rule: IF {Using iframe → Phishing Otherwise → Legitimate

# Domain based Features

## Age of Domain

This feature can be extracted from WHOIS database (Whois 2005). Most phishing websites live for a short period of time. By reviewing our dataset, we find that the minimum age of the legitimate domain is 6 months.

Rule: IF Age Of Domain ≥ 6 months → Legitimate

 { Otherwise → Phishing

## DNS Record

For phishing websites, either the claimed identity is not recognized by the WHOIS database (Whois 2005) or no records founded for the hostname (Pan and Ding 2006). If the DNS record is empty or not found then the website is classified as “Phishing”, otherwise it is classified as “Legitimate”.

Rule: IF{no DNS Record For The Domain → Phishing

Otherwise → Legitimate

## Website Traffic

This feature measures the popularity of the website by determining the number of visitors and the number of pages they visit. However, since phishing websites live for a short period of time, they may not be recognized by the Alexa database (Alexa the Web Information Company., 1996). By reviewing our dataset, we find that in worst scenarios, legitimate websites ranked among the top 100,000. Furthermore, if the domain has no traffic or is not recognized by the Alexa database, it is classified as “Phishing”. Otherwise, it is classified as “Suspicious”.

Website Rank < 100,000 → Legitimate

Rule: IF{ Website Rank > 100,000 → Suspicious

Otherwise → Phish

## PageRank

PageRank is a value ranging from “0” to “1”. PageRank aims to measure how important a webpage is on the Internet. The greater the PageRank value the more important the webpage. In our datasets, we find that about 95% of phishing webpages have no PageRank. Moreover, we find that the remaining 5% of phishing webpages may reach a PageRank value up to “0.2”.

Rule: IF{PageRank < 0.2 → Phishing Otherwise🡪Legitimate

## Google Index

This feature examines whether a website is in Google’s index or not. When a site is indexed by Google, it is displayed on search results (Webmaster resources, 2014). Usually, phishing webpages are merely accessible for a short period and as a result, many phishing webpages may not be found on the Google index.

Rule: IF{Webpage Indexed by Google → Legitimate

Otherwise → Phishing

## Number of Links Pointing to Page

The number of links pointing to the webpage indicates its legitimacy level, even if some links are of the same domain (Dean, 2014). In our datasets and due to its short life span, we find that 98% of phishing dataset items have no links pointing to them. On the other hand, legitimate websites have at least 2 external links pointing to them.

#Of Link Pointing to The Webpage = 0 → Phishing

Rule: IF{#Of Link Pointing to The Webpage > 0 and ≤ 2 → Suspicious

Otherwise → Legitimate

## Statistical-Reports Based Feature

Several parties such as PhishTank (PhishTank Stats, 2010-2012), and StopBadware (StopBadware, 2010-2012) formulate numerous statistical reports on phishing websites at every given period of time; some are monthly and others are quarterly. In our research, we used 2 forms of the top ten statistics from PhishTank: “Top 10 Domains” and “Top 10 IPs” according to statistical-reports published in the last three years, starting in January2010 to November 2012. Whereas for “StopBadware”, we used “Top 50” IP addresses.

 Rule: IF{Host Belongs to Top Phishing IPs or Top Phishing Domains→ Phishin Otherwise → Legitimate



# Steps in the algorithm:

* I will use Machine Learning Model (Decision Tree, K-nearest Neighbor) to identify phishing websites with my dataset.
* In the backend, Python script will detect the features of the entered URL and compare with our trained datasets and provide us the results whether searched URL is phishing site or non-phishing website.

**Software requirement:**

* Windows server
* Python
* Machine Learning.

# Future Scope:

1. Integrate this service with firewall to detect and stop the phishing websites
2. Create an add-on and integrate with Outlook
3. Develop QR code analysis capability to check if it points to a phishing website, as this is one of the trending techniques

**Conclusion:**

The proposed study emphasized the phishing technique in the context of classification, where phishing website is considered to involve automatic categorization of websites into a predetermined set of class values based on several features and the class variable. The ML based phishing techniques depend on website functionalities to gather information that can help classify websites for detecting phishing sites. The problem of phishing cannot be eradicated, nonetheless can be reduced by combating it in two ways, improving targeted anti-phishing procedures and techniques and informing the public on how fraudulent phishing websites can be detected and identified. To combat the ever evolving and complexity of phishing attacks and tactics, ML anti-phishing techniques are essential.

## REFERENCES:

1. Anti-Phishing working (APWG), [https://docs.apwg.org//reports/apwg\_trends\_report\_q4\_2019.pdf](https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf)
2. Jain A.K., Gupta B.B. “PHISH-SAFE: URL Features-Based Phishing Detection System Using Machine Learning”, *Cyber Security*. *Advances in Intelligent Systems and Computing*, vol. 729, 2018,

## Purbay M., Kumar D, “Split Behavior of Supervised Machine Learning Algorithms for Phishing URL Detection”, *Lecture Notes in Electrical Engineering*, vol. 683, 2021,

## Gandotra E., Gupta D, “An Efficient Approach for Phishing Detection using Machine Learning”, *Algorithms for Intelligent Systems*, Springer, Singapore, 2021, <https://doi.org/10.1007/978-981-15-8711-5_12>.

## 5.Hung Le, Quang Pham, Doyen Sahoo, and Steven C.H. Hoi, “URLNet: Learning a URL Representation with Deep Learning for Malicious URL Detection”, *Conference’17*, Washington, DC, USA, arXiv:1802.03162, July 2017.

## 6.Hong J., Kim T., Liu J., Park N., Kim SW, “Phishing URL Detection with Lexical Features and Blacklisted Domains”, *Autonomous Secure Cyber Systems*. Springer, <https://doi.org/10.1007/978-3-030-33432-1_12>.

## 7.J. Kumar, A. Santhanavijayan, B. Janet, B. Rajendran and B. S. Bindhumadhava, “Phishing Website Classification and Detection Using Machine Learning,” *2020 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, 2020, pp. 1–6, 10.1109/ICCCI48352.2020.9104161.

## 8.Hassan Y.A. and Abdelfettah B, “Using case- based reasoning for phishing detection", *Procedia Computer Science*, vol. 109, 2017, pp. 281–288.

1. J. Anirudha and P. Tanuja,”Phishing Attack Detection using Feature Selection Techniques “, Proceedings of International Conference on Communication and Information Processing (ICCIP), 2019, <http://dx.doi.org/10.2139/ssrn.3418542>
2. Wu CY, Kuo CC, Yang CS,” A phishing detection system based on machine learning” In: 2019 International Conference on Intelligent Computing and its Emerging Applications (ICEA), pp 28–32, 2019.
3. Chiew KL, Chang EH, Tiong WK,”Utilisation of website logo for phishing detection”, Computer Security, pp.16–26, 2015.

## Srinivasa Rao R, Pais AR, “Detecting phishing websites using automation of human behavior”, *In: Proceedings of the 3rd ACM workshop on cyber-physical system security*, ACM, pp 33–42, 2017.