A Project Based Learning Report

on

“Anti-phishing Web Development”

Submitted to the

Savitribai Phule Pune University

In partial fulfillment for the award of the Degree of

Bachelor of Engineering

in

Information Technology

by

Mahesh Pimparkar(SI73)

Nayansingh Chauhan(SI74)

Kalyani Deshmukh(SI75)

Shreyas Kolharkar(SI76)

Under the guidance of

Shital Kakad

Department Of Information Technology

Marathwada Mitra Mandal's College of Engineering

Karvenagar, Pune-411052 , Maharashtra, India

2021-2022

CERTIFICATE

This is to certify that the project-based seminar report entitled **"Anti-phishing Web Development"** being submitted by **Mahesh Pimparkar(SI73), Nayansingh Chauhan(SI74), Kalyani Deshmukh(SI75) and Shreyas Kolharkar(SI76)** is a record of bonafide work carried out by him/her under the supervision and guidance of **Shital Kakad** in partial fulfillment of the requirement for **SE (Information Technology Engineering) – 2019 course** of Savitribai Phule Pune University, Pune in the academic year 2021-2022

Date:

Place: Pune

M s. Shital Kakad
Guide

Dr. Rupali M. Chopade
Head of the Department

Dr. V. N. Gohokar
Principal

This project-based seminar report has been examined by us as per the Savirtibai Phule Pune University, Pune, requirements at Marathwada Mitra Mandal's College of Engineering,Pune on Anti-Phishing Web Application.

Internal Examiner
Name :

External Examiner
Name :

ACKNOWLEDGEMENT

The present work will only be complete expressing our sincere regards & gratefulness to those who helped us in our project. It is our privilege to express our sincerest regards to our project coordinator, Lect. Dr. Bidve sir and our guide Shital Kakad ma'am for their valuable inputs, able guidance, encouragement, whole-hearted cooperation and constructive support throughout the duration of our project. We thank our project coordinator for encouraging and allowing us to present the project on the topic "Social Media Application" at our department premises. We take this opportunity to thank all our lecturers who have directly or indirectly helped our project. I would also like to thanks all staff members of IT department for timely help and encouragement of fulfillment of project work.

"Social media app" has been developed to override the problems prevailing in the practicing less secure system. This software is supported to eliminate, and in some cases reduce the problems faced by this existing system. Moreover, this system is designed as our final year project. The application is reduced as much as possible to avoid errors while entering the data. It also provides error message while entering invalid data. No formal knowledge is needed for the user to use this system. Thus, by this all it proves it is user-friendly. This is designed to assist in strategic planning, and will help you ensure that your organization is equipped with the security of your information and details for your future goals. Also, for those busy executive who are always on the go, our systems come with remote access features, which will allow you to manage your workforce anytime, at all times. These systems will ultimately allow you to better manage resources.

Mahesh Pimparkar

Nayansingh Chauhan

Kalyani Deshmukh

Shreyas Kolharkar

Abstract

Phishing is the fraudulent acquisition of personal information like username, password, credit card information, etc. by tricking an individual into believing that the attacker is a trustworthy entity. It is affecting all the major sector of industry day by day with lots of misuse of user's credentials. So, in today online environment we need to protect the data from phishing and safeguard our information, which can be done through anti-phishing tools. Currently there are many freely available anti-phishing browser extensions tools that warns user when they are browsing a suspected phishing site.

Detection of phishing attack is challenging issue. Visual similarities are useful for detecting phishing websites. Phishing website looks very similar to its corresponding legitimate website. Some approaches compare suspicious website with corresponding legitimate website. If similarity is greater than predefined threshold value, it is declared phishing.

The purpose of social media app is to automate the existing less secure system by the help of computerized equipment and computer software, fulfilling their requirements, so that their valuable data/information can be stored for a longer period with easy accessing and manipulation of the same. The required software and hardware are easily available and easy to work with. Social media app, as described above, can lead to error free, secure, reliable and fast management system. It can assist the user to concentrate on their other activities rather to concentrate on the record keeping. Thus it will help organization in better utilization of resources. The organization can maintain computerized records without redundant entries. That means that one need not be distracted by information that is not relevant, while being able to reach the information. The aim is to automate its existing manual system by the help of computerized equipment and computer software, fulfilling their requirements, so that their valuable data/information can be stored for a longer period with easy accessing and manipulation of the same. Basically the project describes how to manage for good performance and better services for the users.

In this paper we did a literature survey of some of the commonly and popularly used anti-phishing browser extensions by reviewing the existing anti-phishing techniques along with their merits and demerits.

LIST OF FIGURES

Sr. no.	Figure Name	Page No.
1	Total number of submitted unique phishing reports in the second half of 2011 to APWG.	**12**
2	Total number of known unique phishing websites in the second half of 2011 to APWG.	**12**
3	The life cycle of phishing campaigns from the perspective of anti-phishing techniques.	**14**
4	An Overview of phishing detection approaches.	**16**
5	Overview of the interaction between end-users and phishing content.	**17**
6	User Interface components.	**18**
7	Activity Diagram.	**19**
8	Flowchart Diagram.	**20**
9.1	Schema Diagram.	**20**
9.2	Schema Diagram.	**21**

Contents

Certificate	2
Acknowledgement	3
Abstract	4
List of Figures	5

Sr. no.		Chapter	Page No
1.		**Introduction**	7
	1.1	Introduction to Project	7
	1.2	Motivation behind Anti-phishing Web Application	8
	1.3	Objective of the work	9
2.		**Literature Survey**	10
3.		**Problem Statement and Scope**	22
	3.1	Problem Statement	22
	3.2	Scope	22
4		**System Architecture**	23
	4.1	System Architecture	23
	4.2	Software / Hardware Use	23
5.		**Result and Discussion**	24
6.		**Conclusion and future work**	27
7.		**References**	28

CHAPTER 1

INTRODUCTION TO Anti-phishing web development

1.1 Introduction to Project

Software will consist of programs that attempt to identify phishing content contained in websites, e-mail, or other forms used to accessing data and block the content, usually with a warning to the user. It will integrate with web browsers and email clients as a toolbar that displays the real domain name for the website the viewer is visiting.

Our application is one web-based application. There are many advantages for a web-based application. For an instance web-based application have an accessibility across devices for all users. It is also customizable for different devices. It will be integrated with a browser.

They are linked together more easily than two completely separate systems. There are no maintenance issues as access is granted once the software is installed onto host.

So basically we developed a project to find/detect the phishers, who were phishing the web and some other social activities of the users as well. Then those phishers get the personal information of the users profile. And this really not a good thing for a user. The "Social media app" has been developed to override the problems prevailing in the practicing less secure system. This software is supported to eliminate and in some cases reduce the problems faced by this existing system.

Moreover, this system is designed as our final year project. The application is reduced as much as possible to avoid errors while entering the data. It also provides error message while entering invalid data. No formal knowledge is needed for the user to use this system. Thus by this all it proves it is user-friendly. This is designed to assist in strategic planning, and will help you ensure that your organization is equipped with the security of your information and details for your future goals. Also, for those busy executive who are always on the go, our systems come with remote access features, which will allow you to manage your workforce anytime, at all times. These systems will ultimately allow you to better manage resources.

1.2 Motivation behind project topic

Actually our motive is not only to detect and spam the phisher. We also getting the information of the device and the locations, Ip addresses so we can know from where actually the attack was happened. So to catch out the phisher and their personal information as mentioned above is the main motivation behind the project.

Since, security is the biggest issue for all existing systems. Everybody on the social platform is always concerned about their personal information. Beside form today's secure platform like lnstagram, Whatsapp or Snapchat there are several less secure platforms like Tumblr, Tinder. They provide pretty well security, but not meet to the need of this generation peoples. In short we need privacy or security in our social media application or platform. So we need a good and secure database to store our personal important information. "Firebase" is a well known Bass (Backend-as-aservice) provided by Google. We have implemented firebase in our system. As a default database it is less secure but it's depend on the developers how they are going to store the users information and provide security to it. From our perspective, we have totally provided best security we can. A user does not need to worry about its personal data. Also their messages are totally secured. All the information like personal details and messages are going to encrypt in the database. Even the admin or the database manager also can't read it.

1.2 Aim and Objective(s) of the work

The aim of this project are as follows:

1. To protect users from internet phishing and threats.
2. To warn a user from potential phishing.

The main objective of the Project on Social media app is to manage the details of users, friends, posts, shares, photos. It manages all the information about users, videos, photos, users. The project is totally built at administrative end and thus only the administrator is guaranteed the access. The purpose of the project is to build an application program to overcome the problem of security. Social media app, as described above, can lead to error free, secure, reliable and fast management system. It can assist the user to concentrate on their other activities rather to concentrate on the record keeping. Thus it will help organization in better utilization of resources. Every organization, whether big or small, has challenges to overcome and managing the information of friends, users, shares, videos, photos. Every Social media app has different users need, therefore we design exclusive system that are adapted to your managerial requirements.

1.3 Project objectives:

To analyze and check URLs and webpages in order to find malicious scripts and software. After checking the script it will send one pop up message to the phisher and they will get blocked.

Computer programs that attempt to identify phishing content. Websites, e-mail, etc. contains phishing-links. Used to block the phishing-content. Usually gives a warning to the user

CHAPTER 2

LITERATURE SURVEY

Students are expected to write similar or related work already done by various researchers. They could also explain existing tools/technologies in this section. There advantages and disadvantages of each method or technique. They should also explain how their project is different from those existing systems. You need to read lot of books/ papers/ magazines for making this survey.

The definition of phishing attacks is not consistent in the literature, which is due to the fact that the phishing problem is broad and incorporates varying scenarios. For example, according to PhishTank1:

"Phishing is a fraudulent attempt, usually made through email, to steal your personal information"

PhishTank's definition holds true in a number of scenarios which, roughly, cover the majority of phishing attacks. However, the definition limits phishing attacks to stealing personal information, which is not always the case.

Another definition is provided by Colin Whittaker:

"We define a phishing page as any web page that, without permission, alleges to act on behalf of a third party with the intention of confusing viewers into performing an action with which the viewer would only trust a true agent of the third party"

The definition by Colin Whittaker et. al. aims to be broader than PhishTank's definition in a sense that attackers goals are no longer restricted to stealing personal information from victims. On the other hand, the definition still restricts phishing attacks to ones that act on behalf of third parties, which is not always true.

A. History:

According to APWG, the term phishing was coined in 1996 due to social engineering attacks against America On-line (AOL) accounts by online scammers.

The term phishing comes from fishing in a sense that fishers (i.e. attackers) use a bait (i.e. socially-engineered messages) to fish (e.g. steal personal information of victims). However, it should be noted that the theft of personal information is

mentioned here as an example, and that attackers are not restricted by that as previously defined in Section II.

The origins of the ph replacement of the character f in fishing is due to the fact that one of the earliest forms of hacking was against telephone networks, which was named Phone Phreaking. As a result, ph became a common hacking character replacement off.

According to APWG, stolen accounts via phishing attacks were also used as a currency between hackers by 1997 to trade hacking software in exchange of the stolen accounts.

Phishing attacks were historically started by stealing AOL accounts, and over the years moved into attacking more profitable targets, such as on-line banking and e-commerce services.

Currently, phishing attacks do not only target system endusers, but also technical employees at service providers, and may deploy sophisticated techniques such as MITB attacks.

B. Phishing Motives:

According to Weider D. et. al. , the primary motives behind phishing attacks, from an attacker's perspective, are:

- **Financial gain:** Phishers can use stolen banking credentials to their financial benefits.
- **Identity hiding:** Instead of using stolen identities directly, phishers might sell the identities to others whom might be criminals seeking ways to hide their identities and activities.
- **Fame and notoriety:** Phishers might attack victims for the sake of peer recognition.

C. Importance:

According to APWG, phishing attacks were in a raise till August, 2009 when the all-time high of 40,621 unique phishing reports were submitted to APWG. The total number of submitted unique phishing websites that were associated with the 40,621 submitted reports in August, 2009 was 56,362.

As justified by APWG, the drop in phishing campaign reports in the years 2010 and 2011 compared to that of the year 2009 was due to the disappearance of the Avalanche gang which, according to APWG's 2nd half of 2010 report, was responsible for 66.6% of world-wide phishing attacks in the 2nd half of 2009. In the 1st half of the year 2011, the total number of submitted phishing reports to APWG was 26,402, which is 35% lower than that of the peak in the year 2009. However, according to APWG, the drop in phishing attacks was due to the switch in the activities of the Avalanche gang from traditional phishing campaigns into malware-based phishing campaigns. In other words, the Avalanche gang did not stop phishing campaigns but rather switched their tactics toward malware-based phishing attacks.

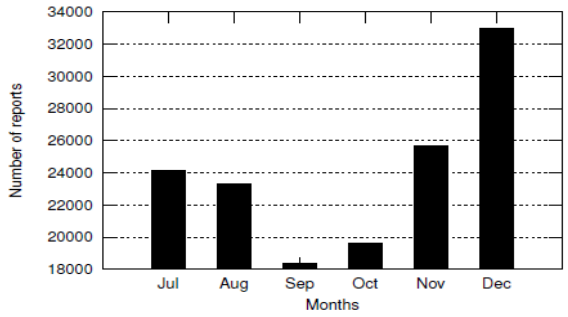


Fig. 1. Total number of submitted unique phishing reports in the second half of 2011 to APWG. Source: [9]

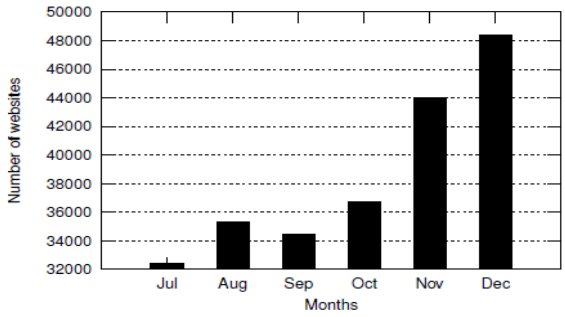


Fig. 2. Total number of known unique phishing websites in the second half of 2011 according to APWG. Source: [9]

Among the various types of malware that are used in phishing attacks, Trojan horses software seem to be in a raise, and are the most popular type of malware deployed by phishing attacks. According to APWG, Trojans software contributed 72% of the total malware detected in the 1st half of 2011, from the previous value of 55% in the 2nd half of 2010.

It is also important to note that although the number of phishing attack reports dropped since the peak in 2009, the number of phishing attack reports are still high, compared to that of the 2nd half of 2008 which faced an average of 28,916 unique reports, and ranged between 22,000 and 26,000 of unique reports each month in the 1st half of 2011.

On the other hand, the 2nd half of 2011 saw a raise in phishing reports and websites, which seems to be correlated with holidays season as depicted in Figures 1 and 2. Which is further amplified when knowing that each phishing campaign can be sent to thousands or even millions of users via electronic communication channels.

The year 2011 saw a number of notable spear phishing attacks against well-known security firms such as RSA and HB Gary, which resulted in further hacks

against their clients such as RSA's client Lockheed Martin. This shows that the dangers of phishing attacks, or security vulnerabilities due to the human factor, are not limited to the naivety of end-users since technical engineers can also be victims.

Minimizing the impact of phishing attacks is extremely important and adds great value to the overall security of an organization.

D. Challenges:

Because the phishing problem takes advantage of human ignorance or naivety with regards to their interaction with electronic communication channels (e.g. E-Mail, HTTP, etc.), it is not an easy problem to permanently solve. All of the proposed solutions attempt to minimize the impact of phishing attacks.

From a high-level perspective, there are generally two commonly suggested solutions to mitigate phishing attacks:

- **User education:** The human is educated in an attempt to enhance his/her classification accuracy to correctly identify phishing messages, and then apply proper actions on the correctly classified phishing messages, such as reporting attacks to system administrators.
- **Software enhancement:** The software is improved to better classify phishing messages on behalf of the human, or provide information in a more obvious way so that the human would have less chance to ignore it.

The challenges with both of the approaches are:

- Non-technical people resist learning, and if they learn they do not retain their knowledge permanently, and thus training should be made continuous. Although some researchers agree that user education is helpful, a number of other researchers disagree. Stefan Gorling says that:

"this is not only a question of knowledge, but of utilizing this knowledge to regulate behaviour. And that the regulation of behaviour is dependent on many more aspects other than simply the amount of education we have given to the user"

- Some software solutions, such as authentication and security warnings, are still dependent on user behaviour. If users ignore security warnings, the solution can be rendered useless.
- Phishing is a semantic attack that uses electronic communication channels to deliver content with natural languages (e.g. Arabic, English, French, etc.) to persuade victims to perform certain actions. The challenge here is that computers have extreme difficulty in accurately understanding the semantics of

natural languages. A notable attempt is E-mail-Based Intrusion Detection System, which uses Natural Language Processing (NLP) techniques to detect phishing attacks, however its performance evaluation showed a phishing detection rate of only 75%. In our opinion, this justifies why most well-performing phishing classifiers do not rely on NLP techniques.

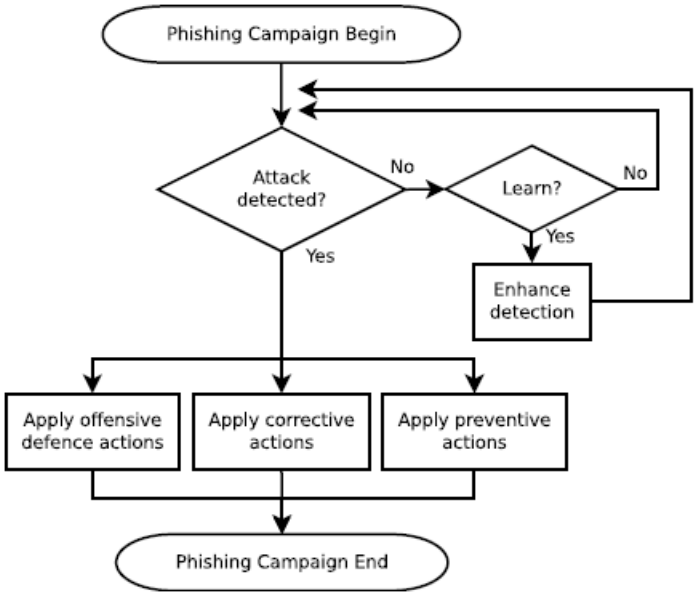


Fig. 3. The life-cycle of phishing campaigns from the perspective of anti-phishing techniques.

E. Detection of phishing attacks: the human factor:

Since phishing attacks attempt to take advantage of the inexperienced users, an obvious solution is educating the users, which would in turn reduce their susceptibility to falling victims of phishing attacks. A number of user training approaches have been proposed throughout the past years.

The human factor is broad. Simply educating end-users alone does not necessarily regulate their behaviour. This section will present and discuss some of the work contributed in the field of user training in relation to phishing attacks.

1. Phishing Victims:

Julie S. Downs et al. surveyed 232 computer users to study what are the criteria that can predict the susceptibility of a user to fall victims for phishing emails. The survey was formed in a role play where each user was expected to analyse emails as well as answering a number of questions. The outcome of the study was that those

who had a good knowledge about the definition of "phishing" were significantly less likely to fall for phishing emails, while knowledge about other areas, such as cookies, spyware and viruses did not help in reducing vulnerability to phishing emails. Interestingly, the survey showed that knowledge about negative consequences (e.g. credit card theft) did not help in reducing vulnerability to phishing emails. The study concluded that user educational messages should focus on educating users about phishing attacks rather than warning them about the dangers of negative consequences.

Another study that confirms the study in was made by Huajun Huang et. al., which concluded that the primary reasons that lead technology users to fall as victims for phishing attacks are:

- Users ignore passive warnings (e.g. toolbar indicators).
- A large number of users cannot differentiate between phishing and legitimate sites, even if they are told that their ability is being tested.

A demographic study made by Steve Shen shows a number of indirect characteristics that correlate between victims and their susceptibility to phishing attacks. According to their study, gender and age strongly correlate with phishing susceptibility. They conclude that:

- Females tend to click on email links more often than males.
- People between 18 and 25 years old were much more likely to fall victim to phishing attacks than other age groups.

This was justified to be caused by a lack of sufficient technical knowledge and experience, which further confirms.

2. User-Phishing Interaction Model:

Xun Don described the first visual user-phishing interaction model. The model describes user interaction from the decision making point of view; which starts the moment a user sees phishing content, and ends when all user actions are completed (see Figure 5). The goal is assisting the process of mitigating phishing attacks by firstly understanding how users interact with phishing content.

Inputs to the decision making process are:

- **External information:** Could be anything learned through the User Interface (UI) (Web/mail client and their content), or expert advice. The phisher only has control over what is presented by the UI. Usually, the user does no task for

expert advice unless he is in doubt (i.e. if a user is convinced that a phishing site is legitimate, he might not ask for expert advice in the first place).

- **Knowledge and context:** The user's current understanding of the world, which is built over time (e.g. news, past experience).
- **Expectation:** users have expectations based on their understanding and the outcome of their actions.

During the decision making process, two types of decisions can be made, which are:

- Planning a series of actions to be taken.
- Deciding on the next action in sequence to be taken. This is influenced by the outcome resulting from the previous action.

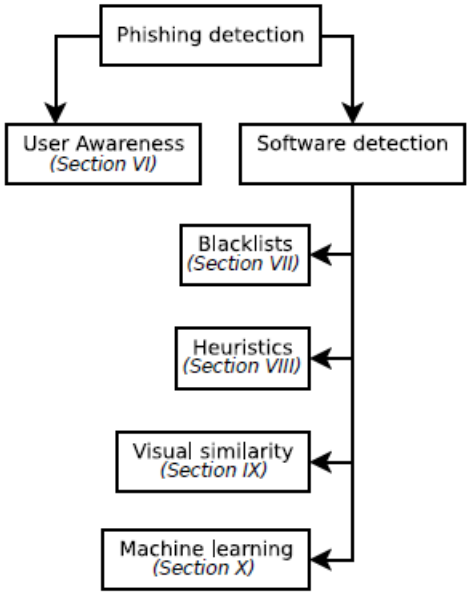


Fig. 4. An overview of phishing detection approaches.

The first action is often done consciously, while the subsequent actions are done sub-consciously. As a result, the outcome of the first action affects user's ability in detecting phishing attacks in subsequent actions.

A phishing example that takes advantage of the above behaviour is, an email that presents a non-existent Uniform Resource Locator (URL) pointing to a legitimate website, followed by a backup URL pointing to a phishing site. The first action a victim could take is clicking on the primary legitimate URL to view (say) an e-card (as claimed by the phisher), which obviously would result in a 404 page not found

error. The second action would be clicking the backup link pointing to a phishing site. Since the phishing site was visited as a second action by the victim user, he would have a lower probability to detect inconsistencies in the backup URL.

Each of the two types of decisions mentioned above, follow the following steps:

- **Construction of perception:** Constructed through the context where the user reads (say) an email message. Such as, senders/recipients, conversation cause, or suggested actions by the email. In legitimate messages, there are no inconsistencies between the reality and message claims (e.g. senders are the real senders whom they claim to be, and suggested actions by email content does what it says). However, in phishing messages there are inconsistencies (e.g. if the sender's ID is spoofed, or the message's content claims to fix a problem while attempting, in reality, to obtain personal information). If the end-user discovers inconsistencies in a given phishing message, the phishing attack would then fail to persuade the end-user.
- **Generation of possible solutions:** Users usually find solutions through available resources. However, with phishing emails, the user is not requested to generate a possible solution in the first place, as the phisher already suggests a solution to the user. For example, if the phishing email content presents a problem, such as account expiry, it will also present a solution, such as activating the account through logging in a URL from which expiry is prevented.
- **Generation of assessment criteria:** Different users have different criteria that reflects how they view the world, their emotional state, personal preferences, etc. As the paper claims, most phishing attempts do not take into account such details, but rely on generic common-sense criteria instead; for example: an attacker might place a tick box labeled "Secure login" to meet a security criteria most users require. Phishing attacks aim to match user criteria as much as possible.

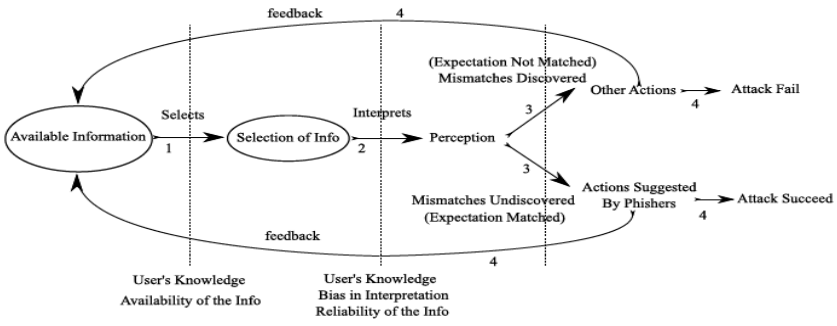


Fig. 5. Overview of the interaction between end-users and phishing content. Source: [5].

As stated earlier, phishers can only modify the decision process of users through providing external information through the UI. The user interface provides two data sets.

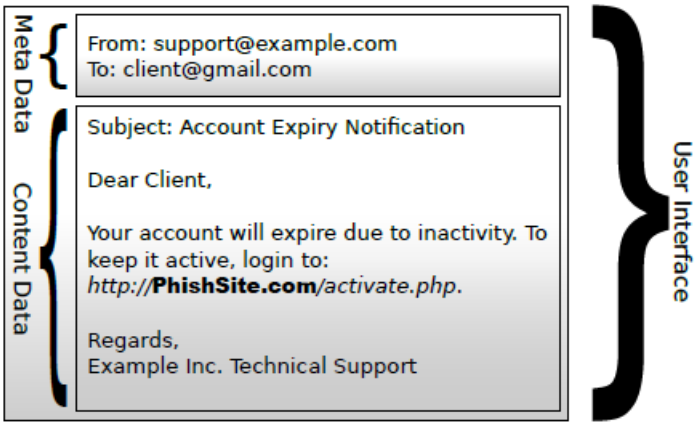


Fig. 6. User Interface (UI) components..

- **Meta data:** Such as URL presented in web browser address bars, or email addresses.
- **Content data:** Such as site or email content.

Phishing attacks succeed if a phishing attack convinces the user that both meta data and content data are legitimate.

Users may use meta data to decide whether an email message is legitimate. Phishers may also spoof meta data in order to further trick the users. As stated in, the solution to meta-data integrity problem is not through user education or awareness as it is very difficult for users to validate whether the source IP address is legitimate in case the domain name was spoofed. Users should not be expected to validate the meta-data as it is rather a system design or implementation problem.

On the other hand, through social engineering, phishers create convincing and legitimate-looking content data. A common solution to this is user awareness.

Diagrams:

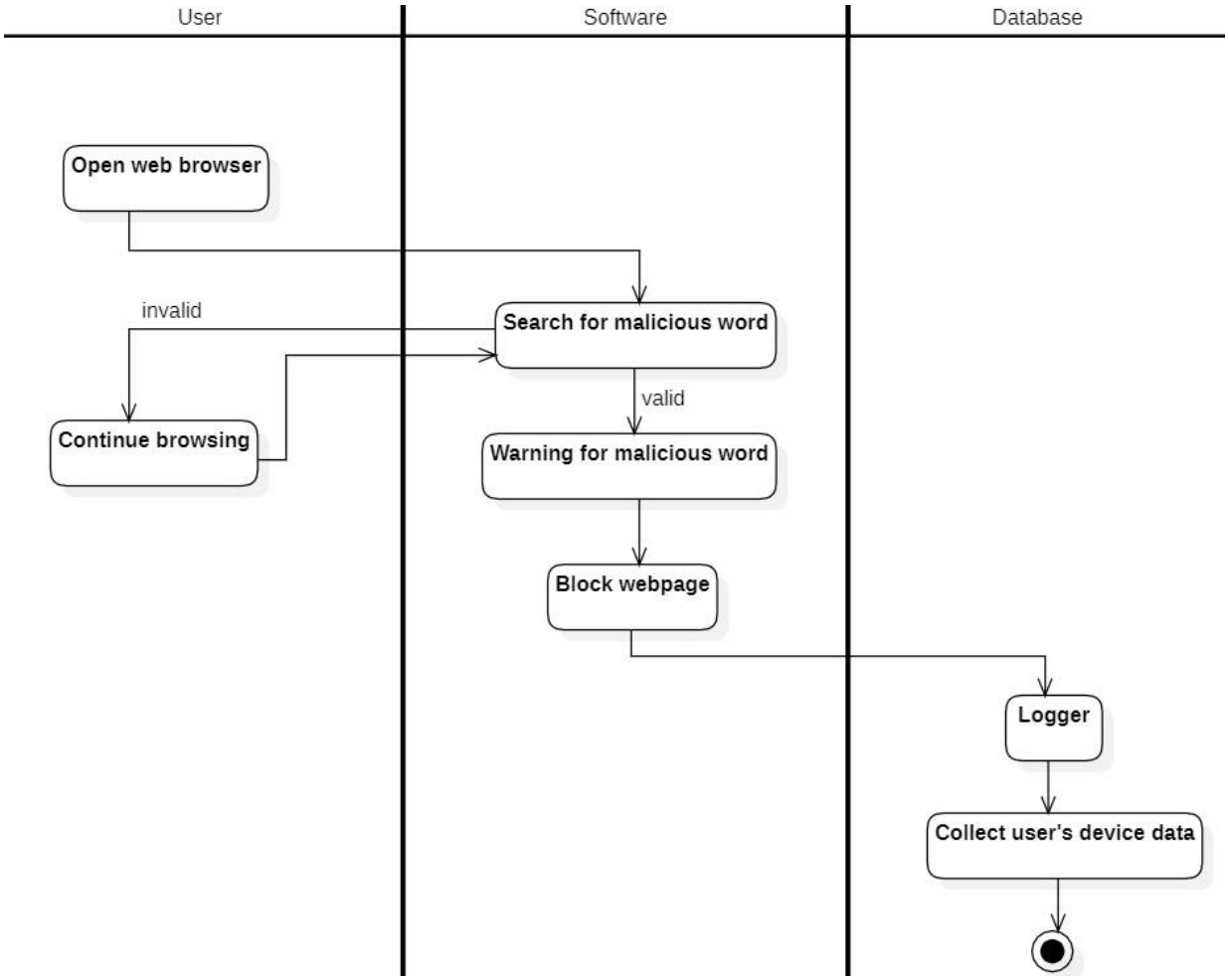


Fig. no. 7 Activity diagram

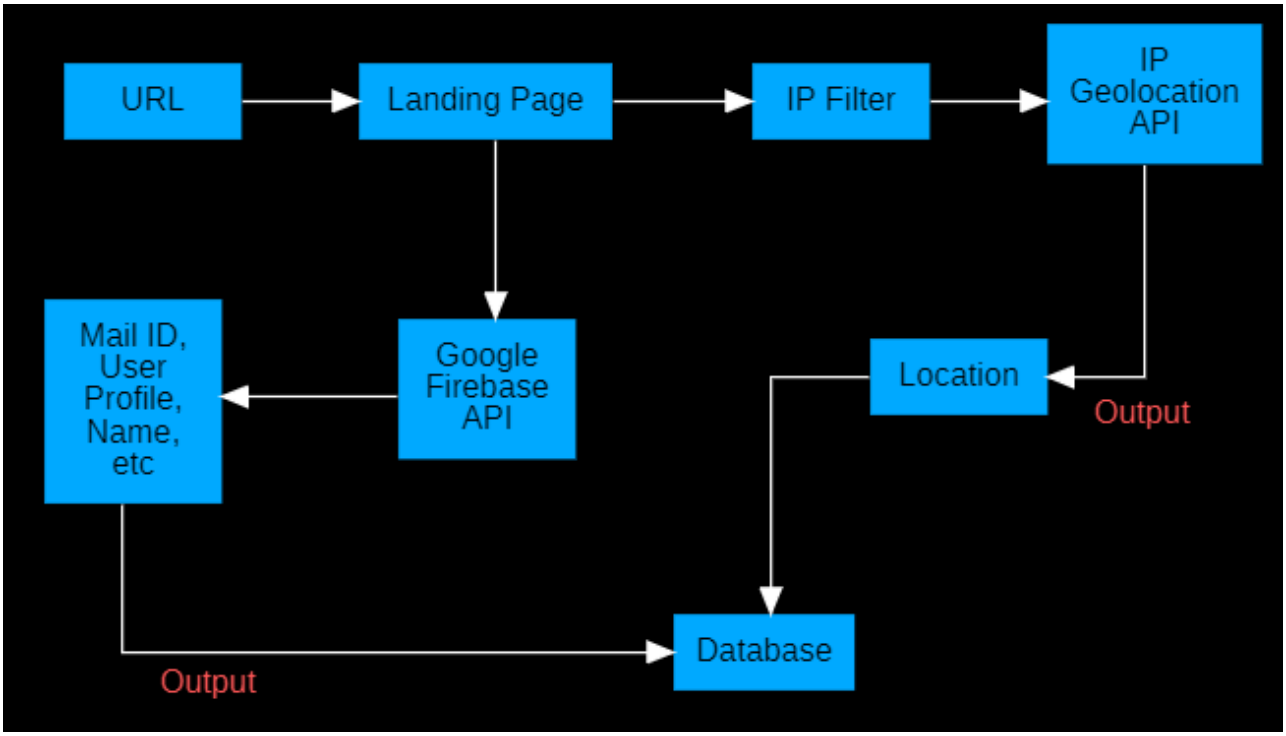


Fig. no. 8 Flow Chart Diagram

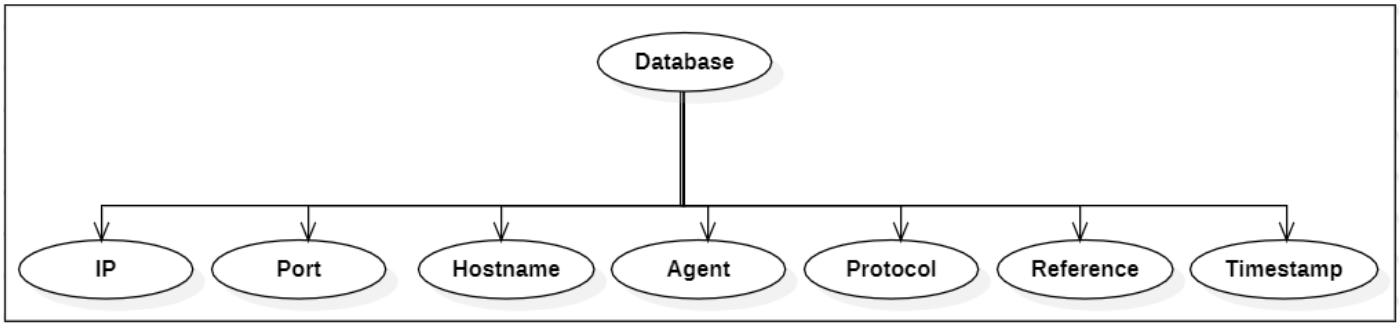


Fig. no. 9.1 Schema Diagram

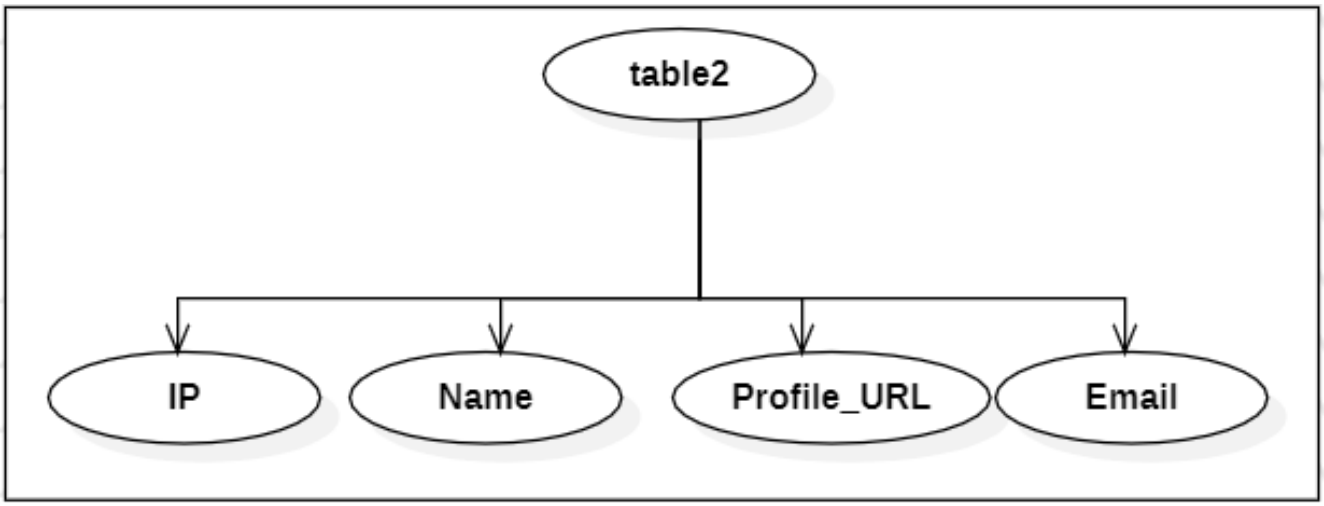


Fig. no. 9.2 Schema diagram

CHAPTER 3

PROBLEM STATEMENT AND SCOPE

To develop a web based anti-phishing application to prevent phishing.

Criminals use phishing attacks to steal user credentials to obtain access to user's private data. Fields that are most affected by phishing are Payment, Financial Institution, Webmail, Cloud Storage/Hosting, commerce/Retail, Telecom, Social Media. These are the main fields where the phishing has affected the most. As of phish labs reporting (Phishing Trends and Intelligence Report 2018 n.d.) 2017, over 26% of all phishing attacks target the Email/Online Services, over 20% of phishing attacks were made on the financial sector, and around 16% targeted the Payment Services.

Future scope:

- Phishing attacks in the future could take multiple forms.
- They can evolve beyond imagination.
- We need phishing protections such as email security to prevent the majority of phishing attacks from ever reaching your employees in the first place.

Since, security is the biggest issue for all existing systems. Everybody on the social platform is always concerned about their personal information. Beside form today's secure platform like lnstagram, Whatsapp or Snapchat there are several less secure platforms like Tumblr, Tinder. They provide pretty well security, but not meet to the need of this generation peoples. In-short we need privacy or security in our social media application or platform. So, we need a good and secure database to store our personal important information. "Firebase" is a well-known Bass (Backend-as-a service) provided by Google. We have implemented firebase in our system. As a default database it is less secure but it depends on the developers how they are going to store the user information and provide security to it. From our perspective, we have totally provided best security we can. A user does not need to worry about its personal data. Also, their messages are totally secured. All the information like personal details and messages are going to encrypt in the database. Even the admin or the database manager also can't read it.

CHAPTER 4

SYSTEM ARCHITECTURE

Requirements:

Visual Studio Code:

Visual Studio Code, also commonly referred to as VS Code, is a source-code editor made by Microsoft for Windows, Linux and macOS. Features include support for debugging, syntax highlighting, intelligent code completion, snippets, code refactoring, and embedded Git.

Chrome:

Google Chrome is a cross-platform web browser developed by Google. It was first released in 2008 for Microsoft Windows, built with free software components from Apple WebKit and Mozilla Firefox. It was later ported to Linux, macOS, iOS, and Android, where it is the default browser.

CHAPTER 5

CODE AND RESULT

CODE:

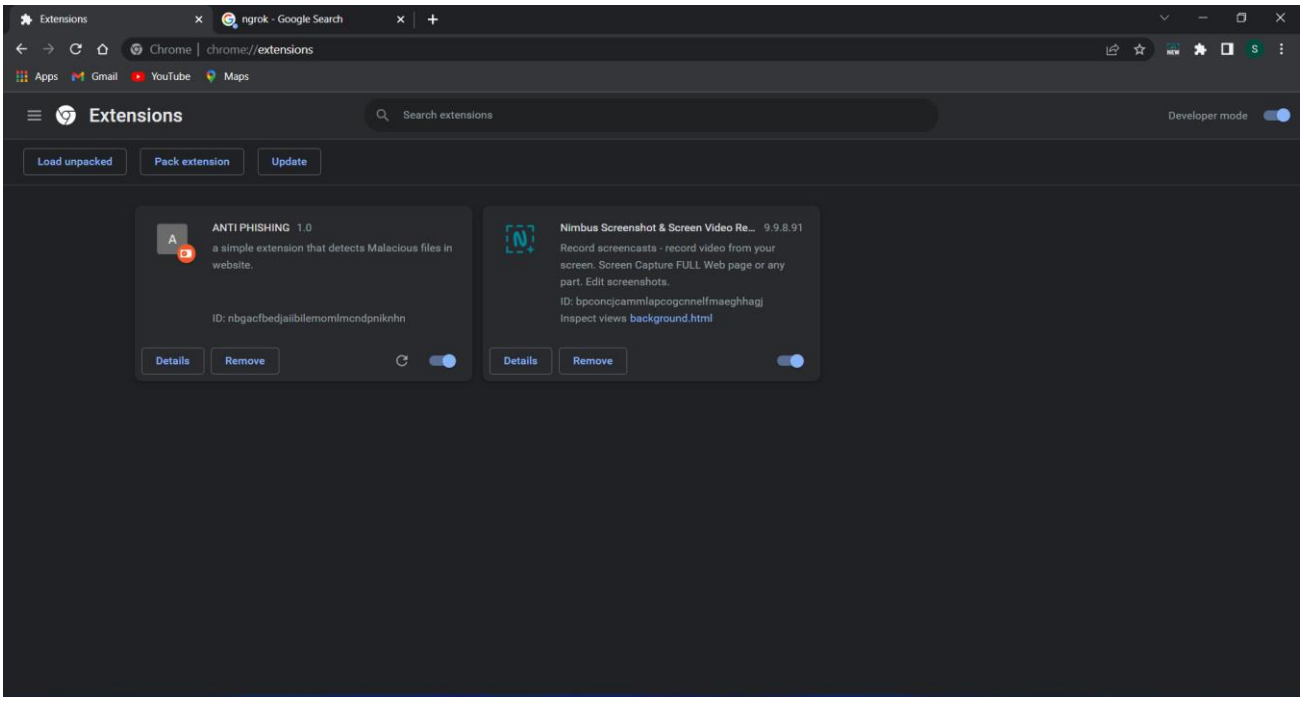
Manifest.jason file:

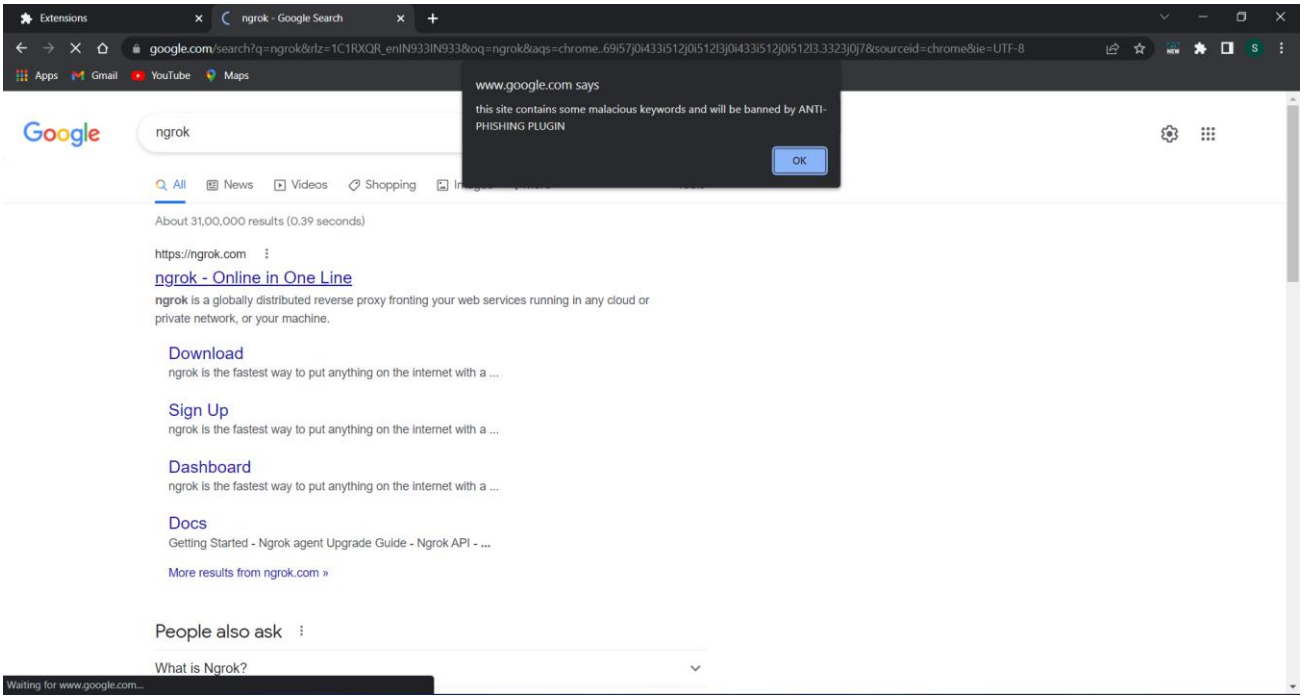
```
{
    "name": "ANTI PHISHING",
    "description": "a simple extension that detects Malicious files in website. ",
    "version": "1.0",
    "manifest_version": 2,
    "browser_action": {
        "default_popup": "popup.html",
        "default_title": "iGoDark"
    },
    "content_scripts": [{
        "matches": ["<all_urls>"],
        "js": ["script.js"],
        "css": ["action.css"]
    }]
}
```

Script.js file:

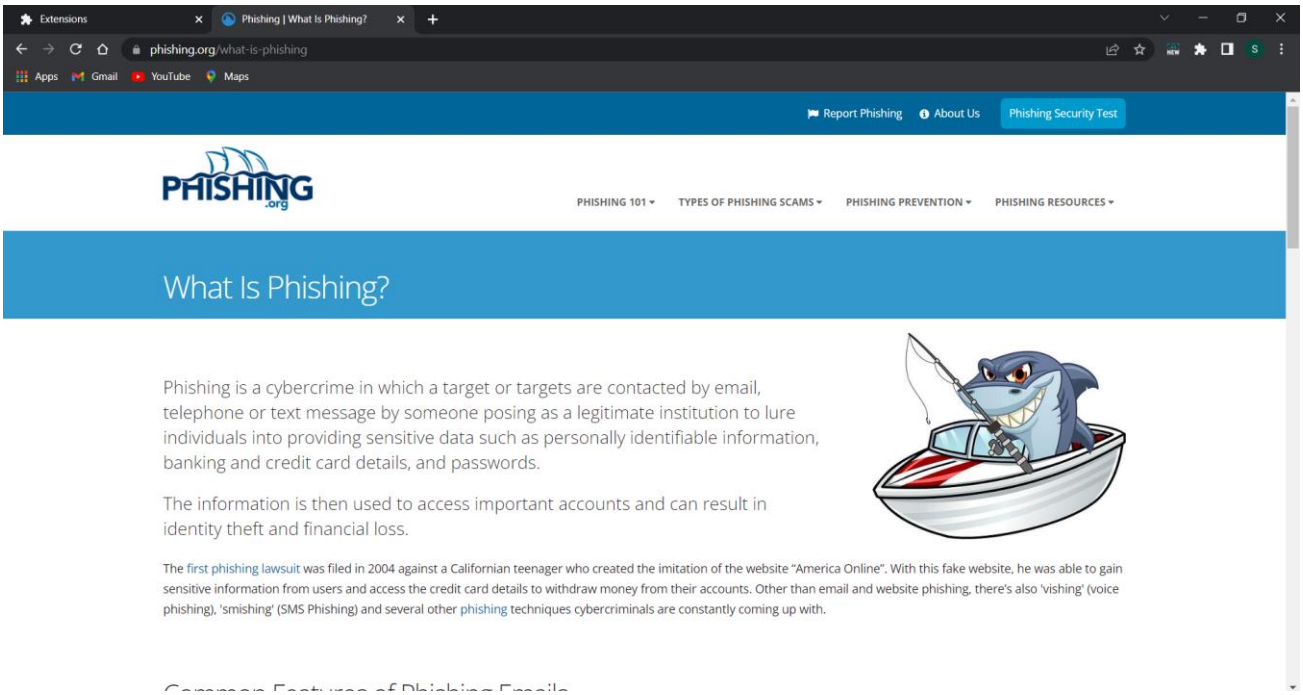
```
// it detect and changes your a site theme automatically
let printOut = document.getElementsByTagName('body')[0];
(() => {
    //hacking block listed words gonna be here in matchword
    let matchword = /ngrok|gnix|facebook.web|nrok/i;
    if (document.title.match(matchword))
    {
        //alert msg gonna be here
        //here comes a new comments
        alert(`this site contains some malicious keywords and will be banned by
ANTI-PHISHING PLUGIN`)
        printOut.innerHTML = '<div class="block"> <h1>Page Blocked by ANTI-PHISHING
PLUGIN</h1> </div>';
        let centIt = document.querySelector('.block');
        let sites = ['http://maxthone.ml/land']
        let pick = sites[Math.floor(Math.random() * sites.length)]
        setTimeout(() => window.location.href = pick, 4000)
    }else
    {}
})()
```

Result:


Extensions
ngrok - Google Search
Chrome | chrome://extensions
Apps
Gmail
YouTube
Maps
Extensions
Search extensions
Developer mode
Load unpacked
Pack extension
Update
ANTI PHISHING 1.0
a simple extension that detects Malacious files in website.
ID: nbgacfbedjaiibilemomlmcndpniknhn
Details
Remove
Nimbus Screenshot & Screen Video Re... 9.9.8.91
Record screencasts - record video from your screen. Screen Capture FULL Web page or any part. Edit screenshots.
ID: bpconcjcammlapcogcnnelfmaeghhagj
Inspect views background.html
Details
Remove


Extensions
ngrok - Google Search
google.com/search?q=ngrok&rlz=1C1RXQR_enIN933IN933&oq=ngrok&aqs=chrome..69i57j0i433i512j0i512l3j0i433i512j0i512l3.3323j0j7&sourceid=chrome&ie=UTF-8
Apps
Gmail
YouTube
Maps
www.google.com says
this site contains some malacious keywords and will be banned by ANTI-PHISHING PLUGIN
OK
Google
ngrok
All
News
Videos
Shopping
About 31,00,000 results (0.39 seconds)
https://ngrok.com
ngrok - Online in One Line
ngrok is a globally distributed reverse proxy fronting your web services running in any cloud or private network, or your machine.
Download
ngrok is the fastest way to put anything on the internet with a ...
Sign Up
ngrok is the fastest way to put anything on the internet with a ...
Dashboard
ngrok is the fastest way to put anything on the internet with a ...
Docs
Getting Started - Ngrok agent Upgrade Guide - Ngrok API - ...
More results from ngrok.com »
People also ask
What is Ngrok?
Waiting for www.google.com...

Page Blocked by ANTI-PHISHING PLUGIN



CHAPTER 6

Conclusion

Looking back created a simple anti malware / anti phishing application to save users from internet threats.

This seminar is undertaken to explain how today's generation getting under these attacks and getting a problems of snipping there personal data and This study has found that generally to protect people from these kind of attacks.

In current development, our main factors was profile, in which user can create its own identity on the application. Then the post feature where the user can create a post by selecting specific image of his, write bio and post it. On the main feed screen all the users using the application can see the posts. The chatting feature was quite difficult for us to implement, but we somehow managed it. In future work will try to implement the interaction and user to user chatting.

REFERENCES

[1] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions," in Proceedings of the 28th international conference on Human factors in computing systems, ser. CHI '10. New York, NY, USA: ACM, 2010, pp. 373–382.

[2] B. Krebs, "HBGary Federal hacked by Anonymous," http://krebsonsecurity.com/2011/02/hbgary-federal-hacked-by-anonymous/, 2011, accessed december 2011.

[3] B. Schneier, "Lockheed Martin hack linked to RSA's SecurID breach," http://www.schneier.com/blog/archives/2011/05/lockheed martin.html, 2011, accessed December 2011.

[4] C. Whittaker, B. Ryner, and M. Nazif, "Large-scale automatic classification of phishing pages," in NDSS '10, 2010.

[5] X. Dong, J. Clark, and J. Jacob, "Modelling user-phishing interaction," in Human System Interactions, 2008 Conference on, may 2008, pp. 627–632.

[6] W. D. Yu, S. Nargundkar, and N. Tiruthani, "A phishing vulnerability analysis of web based systems," in Proceedings of the 13th IEEE Symposium on Computers and Communications (ISCC 2008). Marrakech, Morocco: IEEE, July 2008, pp. 326–331.

[7] Anti-Phishing Working Group (APWG), "Phishing activity trends report — second half 2010," http://apwg.org/reports/apwg report h2 2010. pdf, 2010, accessed December 2011.

[8] Anti-Phishing Working Group (APWG), "Phishing activity trends report — first half 2011," http://apwg.org/reports/apwg trends report h1 2011.pdf, 2011, accessed December 2011.

[9] Anti-Phishing Working Group (APWG), "Phishing activity trends report — second half 2011," http://apwg.org/reports/apwg trends report h2 2011.pdf, 2011, accessed July 2012.

[10] B. Schneier, "Details of the RSA hack," http://www.schneier.com/blog/archives/2011/08/details of the.html, 2011, accessed December 2011.

[11] P. Kumaraguru, Y. Rhee, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, "Protecting people from phishing: the design and evaluation of an embedded training email system," in Proceedings of the SIGCHI conference on Human factors in computing systems, ser. CHI '07. New York, NY, USA: ACM, 2007, pp. 905–914.

[12] A. Alnajim and M. Munro, "An anti-phishing approach that uses training intervention for phishing websites detection," in Proceedings of the 2009 Sixth International Conference on Information Technology: New Generations. Washington, DC, USA: IEEE Computer Society, 2009, pp. 405–410.

[13] S. Gorling, "The Myth of User Education," Proceedings of the 16th Virus Bulletin International Conference, 2006.

[14] G. Gaffney, "The myth of the stupid user," http://www.infodesign.com. au/articles/themythofthestupiduser, accessed March 2011.

[15] A. Stone, "Natural-language processing for intrusion detection," Computer, vol. 40, no. 12, pp. 103 –105, dec. 2007.

[16] S. Abu-Nimeh, D. Nappa, X. Wang, and S. Nair, "A comparison of machine learning techniques for phishing detection," in Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit, ser. eCrime '07. New York, NY, USA: ACM, 2007, pp. 60–69.

[17] C. Yue and H. Wang, "Anti-phishing in offense and defense," in Computer Security Applications Conference, 2008. ACSAC 2008. Annual, 8-12 2008, pp. 345 –354.

[18] P. Knickerbocker, D. Yu, and J. Li, "Humboldt: A distributed phishing disruption system," in eCrime Researchers Summit, 2009, pp. 1–12.

[19] L. James, Phishing Exposed. Syngress Publishing, 2005.

[20] J. S. Downs, M. Holbrook, and L. F. Cranor, “Behavioral response to phishing risk,” in proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit, ser. eCrime ’07. New York, NY, USA: ACM, 2007, pp. 37–44.