



CYBERDEFEND

USER MANUAL

❖ About CyberDefend Platform

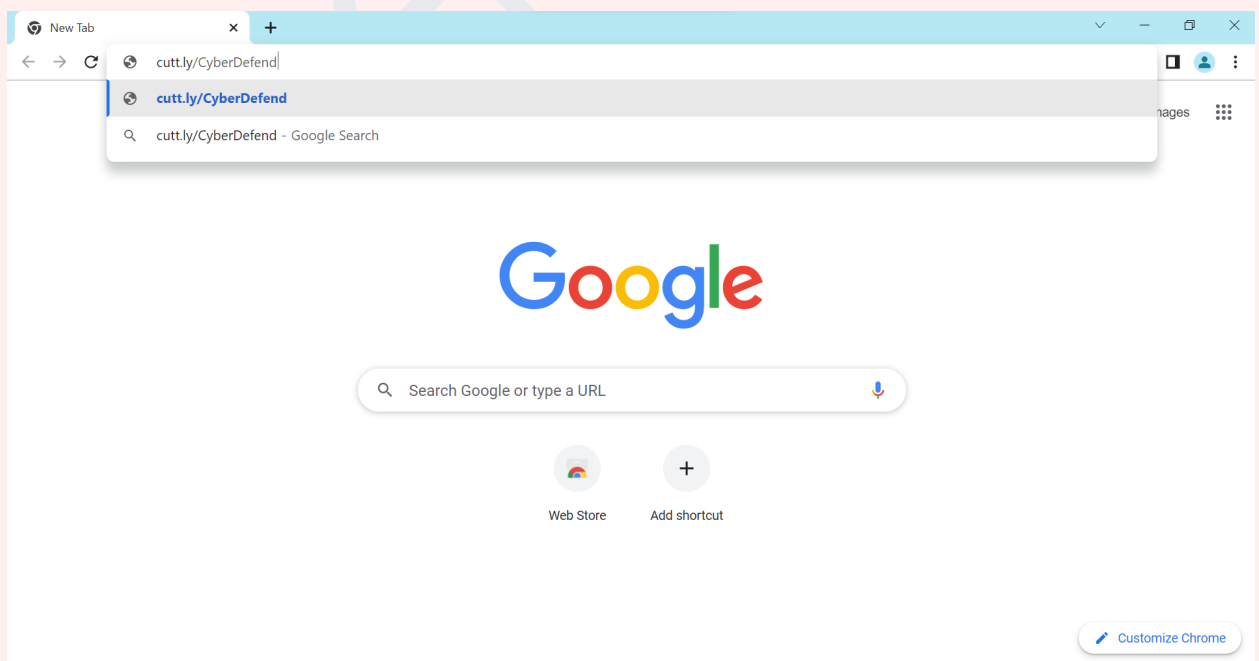
CyberDefend is an intelligent tool that aids the public to detect and prevent common zero-day cyberattacks carried out by the dissemination of spam messages and malicious URLs. It mainly consists of different integral features such as detection of spam messages with build in malicious **URL detector**, **discovery of past visits to malicious websites** and **safe search**.

❖ Intended Audience

This tool is intended to **protect people** who use SMS as a form of communication service from unwanted or malicious messages and also users who would like to gauge the safety of a URL they might have received from an unreliable source or verify their browsing history.

❖ Navigating to CyberDefend Platform

- 1) Open any web browser of your choice and enter URL: <https://cutt.ly/CyberDefend>

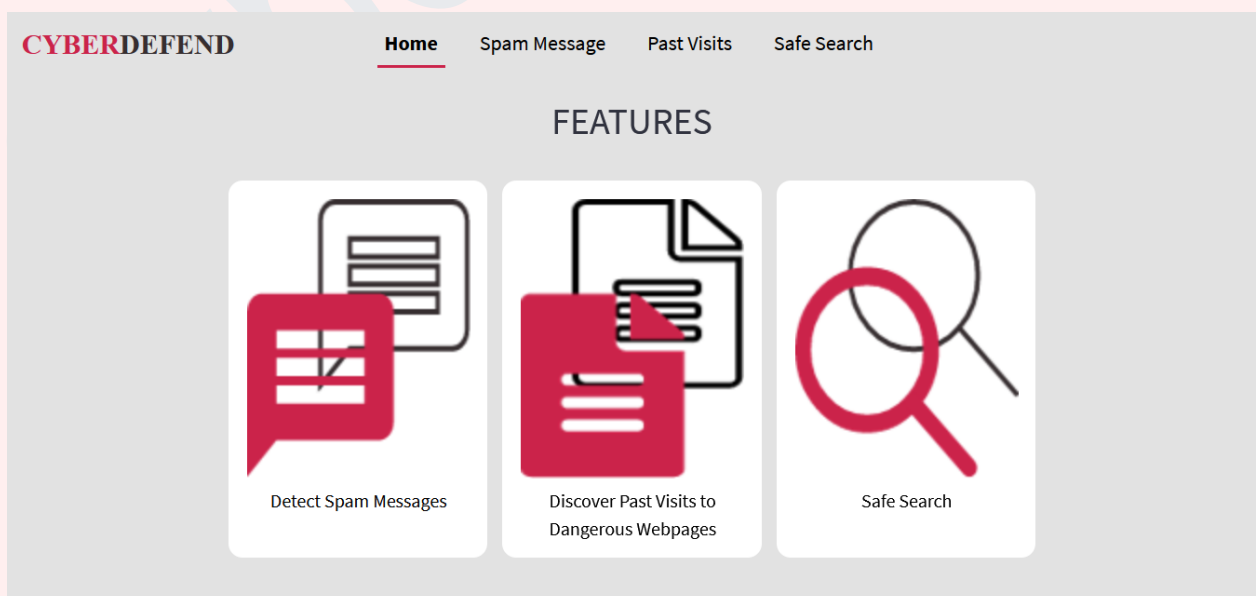


❖ About Homepage

1) Homepage provides a brief description about the platform.

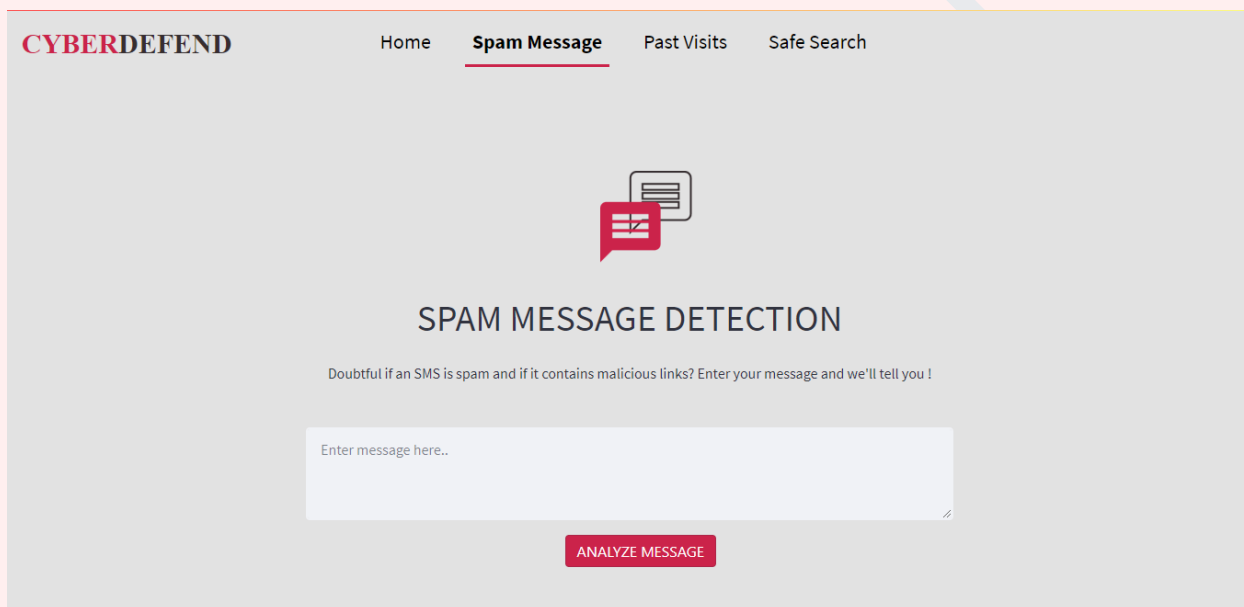


2) Scrolling down provides more information about the features of the web platform



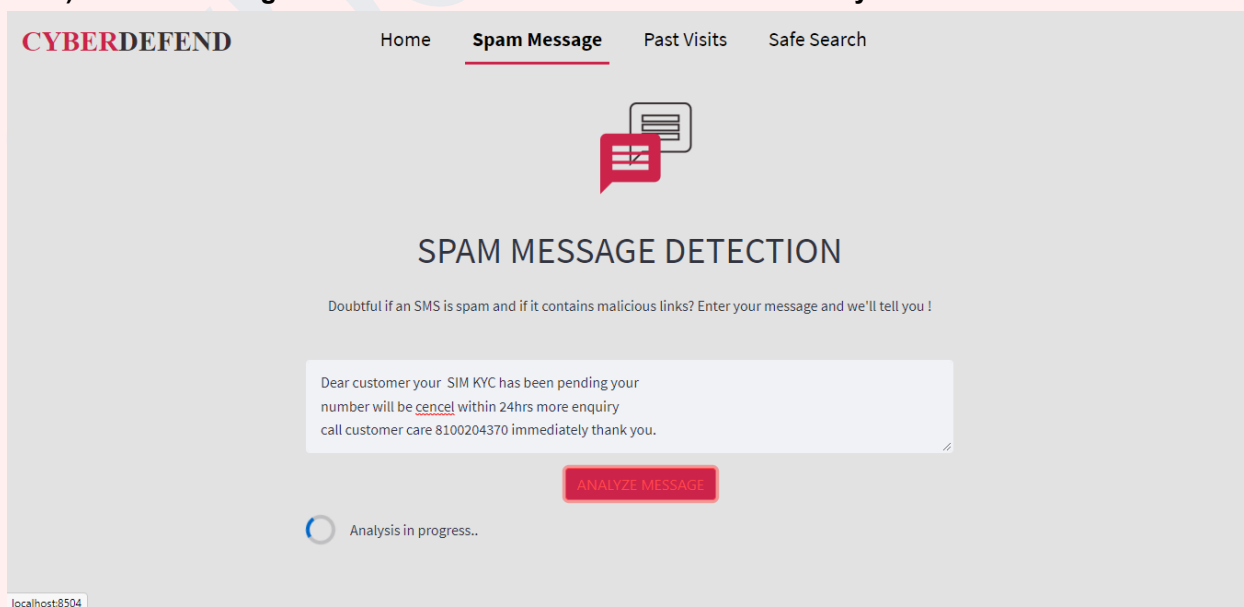
❖ Spam Message Detector

1) Click “Spam Message” tab on the Navigation bar



The screenshot shows the web application interface for the Spam Message Detector. At the top, there is a navigation bar with the logo "CYBERDEFEND" on the left and four tabs: "Home", "Spam Message" (which is underlined), "Past Visits", and "Safe Search". Below the navigation bar, there is a central area with a speech bubble icon containing a checkmark. The title "SPAM MESSAGE DETECTION" is displayed in large, bold, black letters. Below the title, a subtitle reads: "Doubtful if an SMS is spam and if it contains malicious links? Enter your message and we'll tell you !". There is a large, light blue text input field with the placeholder text "Enter message here..". Below the input field is a red button labeled "ANALYZE MESSAGE".

2) Paste message to be checked in the text area and click analyze button



The screenshot shows the web application interface for the Spam Message Detector, similar to the previous one, but with a message pasted into the text input field. The message reads: "Dear customer your SIM KYC has been pending your number will be cancel within 24hrs more enquiry call customer care 8100204370 immediately thank you." Below the input field, the red "ANALYZE MESSAGE" button is visible. At the bottom of the page, there is a loading spinner icon and the text "Analysis in progress..". In the bottom left corner, there is a small text label "localhost:8504".

3) Obtain appropriate results from the classifier

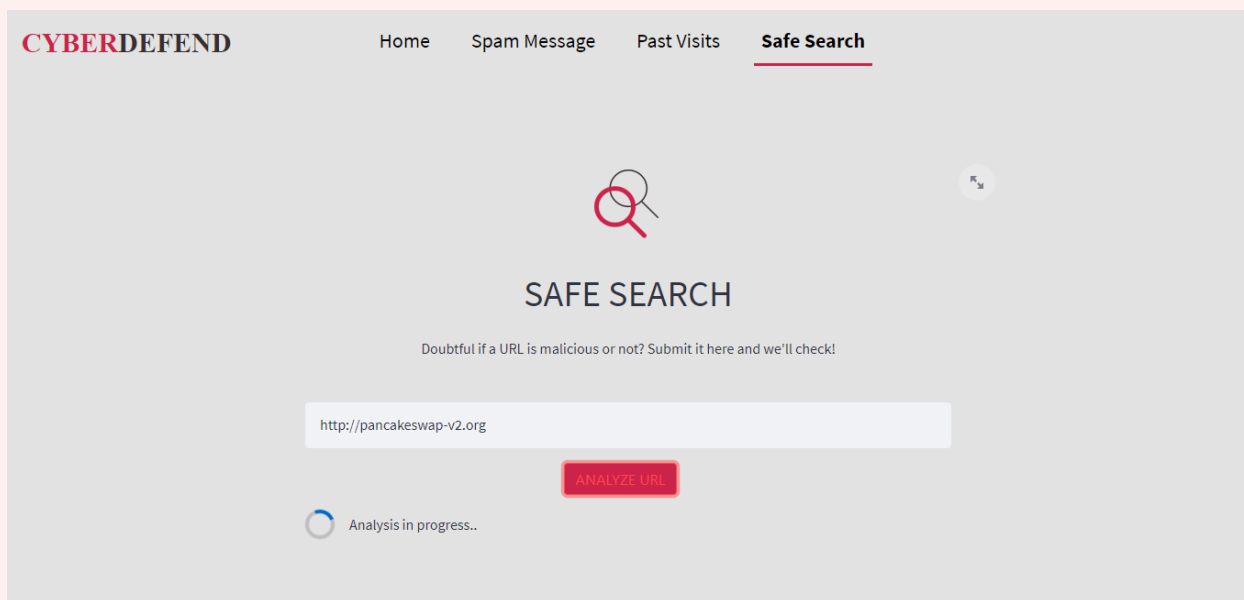
The screenshot shows the 'Spam Message' tab selected in the navigation bar. The main content area displays a sample spam message in a light blue box: "Dear customer your SIM KYC has been pending your number will be cencel within 24hrs more enquiry call customer care 8100204370 immediately thank you." Below the message is a red button labeled "ANALYZE MESSAGE". The result is shown as a red skull and crossbones icon in a white box, followed by the text "Message is SPAM!". Below this, a red box labeled "Message" contains the original spam text: "Dear customer your SIM KYC has been pending your number will be cencel within 24hrs more enquiry call customer care 8100204370 immediately thank you."

❖ Safe Search

1) Click “Safe Search” tab on the Navigation bar

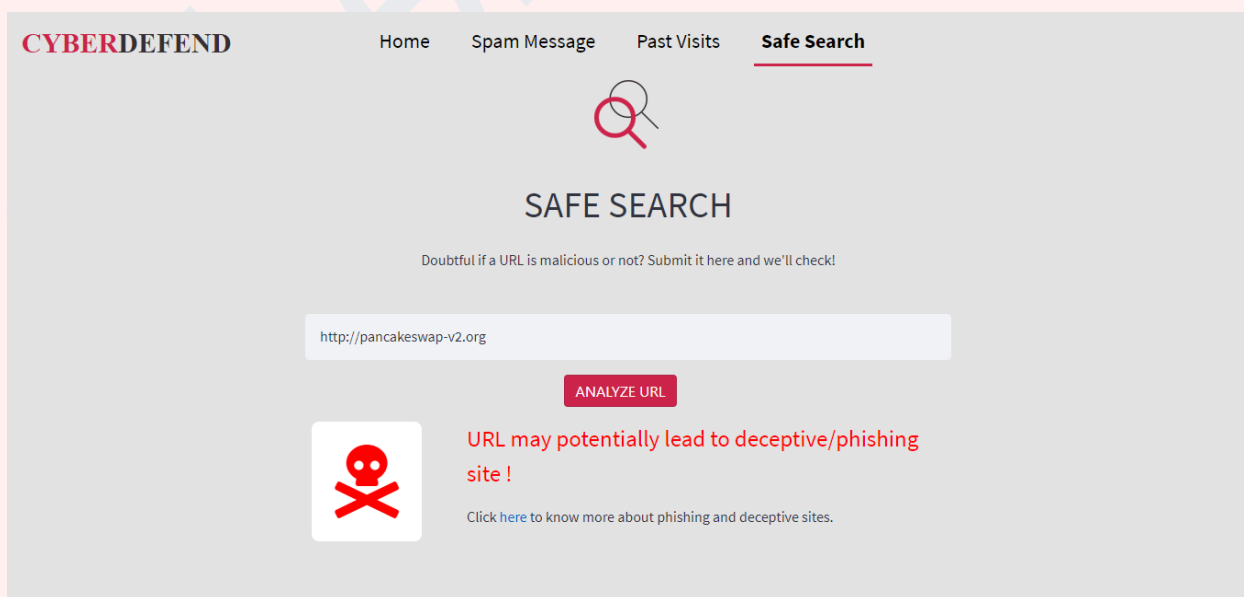
The screenshot shows the 'Safe Search' tab selected in the navigation bar. The main content area features a magnifying glass icon above the text "SAFE SEARCH". Below this is a subtitle: "Doubtful if a URL is malicious or not? Submit it here and we'll check!". A text input field with the placeholder "Enter URL here.." is provided, followed by a red button labeled "ANALYZE URL".

2) Paste URL to be checked in the URL area and click analyze button



The screenshot shows the CYBERDEFEND website's 'Safe Search' page. The navigation bar includes 'Home', 'Spam Message', 'Past Visits', and 'Safe Search' (which is underlined). The main heading is 'SAFE SEARCH' with a magnifying glass icon above it. Below the heading is a subtext: 'Doubtful if a URL is malicious or not? Submit it here and we'll check!'. A text input field contains the URL 'http://pancakeswap-v2.org'. Below the input field is a red button labeled 'ANALYZE URL'. At the bottom left, there is a circular progress indicator and the text 'Analysis in progress..'. A large, faint watermark 'PHISHING' is visible in the background.

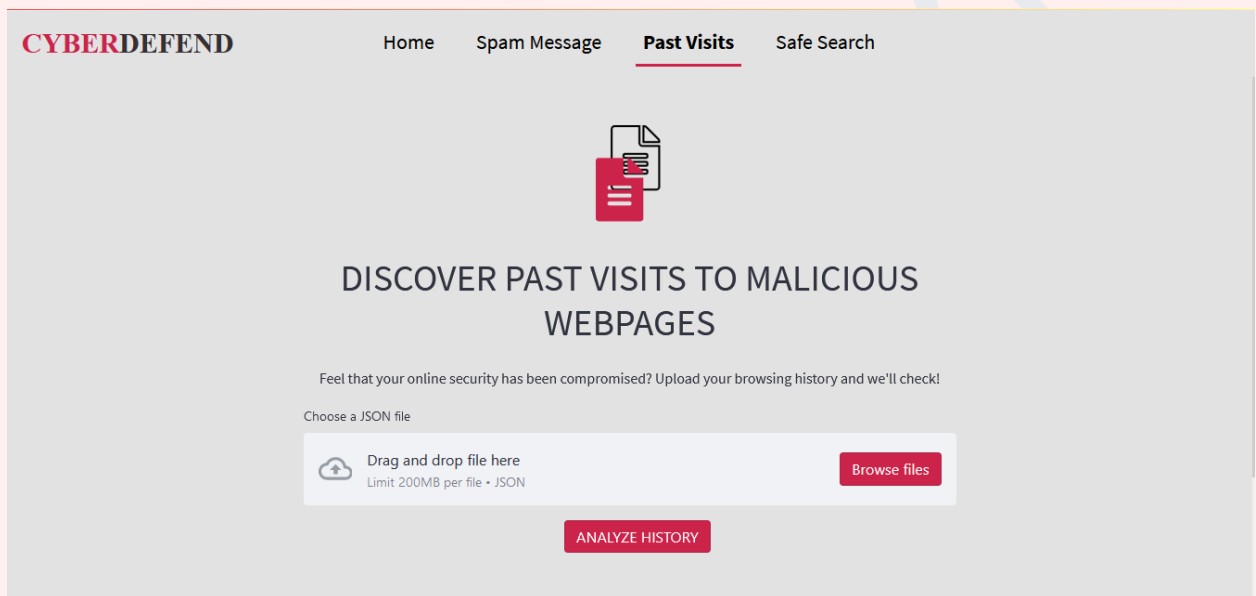
3) Obtain appropriate results from the classifier



The screenshot shows the same CYBERDEFEND 'Safe Search' page, but now with results for the URL 'http://pancakeswap-v2.org'. The 'ANALYZE URL' button is still present. Below the input field, there is a red skull and crossbones icon inside a white square. To the right of the icon, the text reads: 'URL may potentially lead to deceptive/phishing site !'. Below this, a smaller line of text says: 'Click [here](#) to know more about phishing and deceptive sites.' The navigation bar and main heading remain the same. The large, faint watermark 'PHISHING' is still visible in the background.

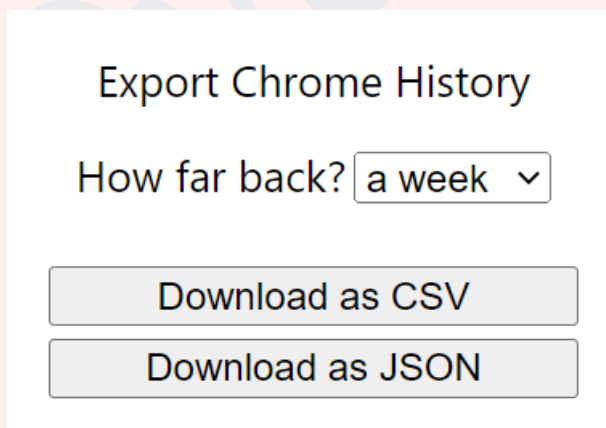
❖ Past Visits

1) Click “Past Visits” tab on the Navigation bar



The screenshot shows the CYBERDEFEND website's 'Past Visits' section. The navigation bar at the top includes 'Home', 'Spam Message', 'Past Visits' (which is underlined), and 'Safe Search'. The main heading is 'DISCOVER PAST VISITS TO MALICIOUS WEBPAGES'. Below this, a subtext reads: 'Feel that your online security has been compromised? Upload your browsing history and we'll check!'. A prompt 'Choose a JSON file' is followed by a drag-and-drop area with the text 'Drag and drop file here' and 'Limit 200MB per file • JSON'. To the right of this area is a red 'Browse files' button. At the bottom center, there is a red 'ANALYZE HISTORY' button.

2) Download your browsing history



The screenshot shows a dialog box titled 'Export Chrome History'. It contains a label 'How far back?' followed by a dropdown menu currently set to 'a week'. At the bottom, there are two buttons: 'Download as CSV' and 'Download as JSON'.

3) Upload the JSON file of browsing history to be checked and click analyze button

The screenshot shows the 'CYBERDEFEND' website with the 'Past Visits' tab selected. The main heading is 'DISCOVER PAST VISITS TO MALICIOUS WEBPAGES'. Below this, a message says 'Feel that your online security has been compromised? Upload your browsing history and we'll check!'. A section titled 'Choose a JSON file' contains a drag-and-drop area with the text 'Drag and drop file here' and 'Limit 200MB per file • JSON'. A 'Browse files' button is to the right. Below the drag-and-drop area, a file named 'history (1).json' (198.0KB) is listed with a close button. An 'ANALYZE HISTORY' button is prominently displayed. At the bottom, a progress indicator shows 'Analysis in progress..'.

4) Obtain appropriate results from the classifier

The screenshot shows the 'CYBERDEFEND' website with the 'Past Visits' tab selected. The 'ANALYZE HISTORY' button is visible. Below it, a large green checkmark icon is displayed next to the text 'Analysis Complete!'. A red banner states 'You have potentially visited malicious pages!'. Below this, a table lists the results:

	Title	URL	Potential (Likely) Category
4	Web app sync	https://webappsync.com/resolve/	Phishing

Below the table, there are three footnotes:

- (*) is Advisory provided by Google. Click [here](#) to know more.
- Click [here](#) to know more about malware.
- Click [here](#) to know more about phishing and deceptive sites.

❖ **Contact Us**

For any query feel free to contact us at:

Gopalkrishna Waja: gopalkrishna.w@somaiya.edu

Gaurang Patil: gaurang.patil@somaiya.edu

Charmee Mehta: charmee.m@somaiya.edu

THANK YOU