Problem Statement 02: AI based Monitoring and Detection of Phishing Domains/URLs related to CSEs

1. General Description:

1.1. Phishing attacks remain one of the most persistent and damaging threats in the cybersecurity landscape. Cybercriminals often register domains that closely resemble Critical Sector Entities (CSEs) in order to deceive users into revealing sensitive information such as login credentials, personal identification data, financial data etc. As these attacks become more sophisticated (non-resemblance to CSE URL, use of Tunnelling Services such as Ngrok, Vercel etc., Lookalike/typosquating domains with no contents hosted/ Parked domains), traditional detection methods are no longer sufficient.

1.2. Phishing Domains/URLs: Fraudulent websites/URLs imitating genuine sites of CSEs. The webpage content in the URL is similar to genuine webpage content but the URL itself may or may not be similar to the genuine URL.

1.3. Suspected Domains: Domain names that are intentionally misspelled to deceive users (e.g., typo-squatting domains etc.). They are majorly parked. That means no content hosted on it. However, at a later stage these parked domains may host content to carry our phishing activities.

2. Problem Statement:

Since Phishing attacks have evolved significantly, posing serious threats to the security of users, especially in the context of sensitive information handled by CSE websites, there is an urgent need for a Scalable, Efficient automated solution to detect and alert Phishing and Suspected (likely to be used for phishing) domains/URLs in near real-time to prevent data breaches, financial losses.

3. Expected Outcome:

3.1. An AI/ML based platform to be developed having preferably a browser-based dashboard for operator which at the backend will have AI/ML based engine to continuously crawl, parse, monitor large pool of data from a number of sources in the cyber space and report phishing/suspected domains/URLs of CSEs. Both Structured and Unstructured data to be crawled from the cyber space for monitoring of newly created phishing/ suspected domains.

3.2. Output to have mapping between CSEs and corresponding Phishing/Suspected domains/URLs.

3.3. Capability to Monitor Suspected Domain: The engine should also have the capability to continuously monitor identified suspected domains for at least 3 months (the duration should be configurable) and report in case the suspected domains host CSEs lookalike content, binary etc.

3.4. The engine to have capability to generate report against each identified phishing/suspected domain/URL with attributes like domain creation date/time, IP/Subnet info, maliciousness information, Registrar information, Registrant

information, ASNs, Country, MX Records, Certificate Transparency information, Screenshots, External Verification Data, etc.) etc.

3.5. Detection of Phishing / Suspected domains created using Internationalized Domain Name (IDN).

3.6. Professional dash board with user friendly UI / UX.

3.7. The solution should preferably be capable of running on an on-premises internet connected infrastructure.

Note:

a. Use of third-party Phishing detection platform / API on threat intelligence etc is prohibited in the solution.

b. The participants should declare all API calls / calls to commercial / third party solutions made within their solutions. The same will be verified during evaluation to confirm non-use of prohibited APIs.

c. For each stage, participant should provide a detailed documentation of the developed solution and its implementation.

d. Participants are free to use any language or development framework (preferably opensource) for the solution.

4. Datasets and Evaluation Methodology:

Important artifacts that may be considered for monitoring the domains/URLs is listed at **Annexure A.** These are just illustrative and not comprehensive**.** Developer may consider other innovative methodologies, if needed to detect if an input domain/URL is phishing/suspected or not.

4.1. Datasets for Stage 1:

4.1.1. **Training Dataset:** Folder "PS02_Training_set.zip" contains file having number of phishing and suspected domains corresponding to 10 identified CSEs for the solution development. It will be released at T0 i.e., 01st Aug 2025. The folder will also have some sample screenshots/images of corresponding phishing pages of these CSEs. The participants are free to use their own resources / data sets for solution development.

4.1.2. **Mock Dataset:** Folder "PS02_Mock_set.zip" to contain both Phishing/Suspected URLs from CSEs. This data set will be kept updated regularly by NCIIPC, which the start-up teams/participants can use to self-evaluate their solution and get the feedback to improve their solution. This update will commence from 1st August till 15th Oct 2025 as and when NCIIPC comes to know about the new Phishing/Suspected domains/URLs corresponding to the 10 identified CSEs.

4.1.3. **Shortlisting Data Set:** PS-02_Shortlisting_set.zip will be made available on 16 Oct 2025 to participants. This will consist of 10 CSEs for which the participants will have to run their solution and submit their results within the given time lines.

4.1.4. **Hold-out dataset:** This set (PS-02_hold-out set.zip) will be made available to Stage I short listed participants during evaluation on 10 Nov 2025. PS-02_hold-out set.zip will have two sub parts. First part "PS-02_hold-out set1" will have names of 10 CSEs (along with their domains) and second part "PS-02_hold-out set2" will have a number of newly created domain names.

4.2. Evaluation Methodology for Stage-1

4.2.1. Start-Ups/Student groups should run their solution to detect Phishing/Suspected domains targeting the 10 CSEs mentioned in shortlisted dataset "PS-02_Shortlisting_set.zip" during 16 Oct 2025 to 31 Oct 2025 and populate their result in their submission set "PS-02_<Application ID>_submission.zip". This submission set will be assessed by NCIIPC against actual detected Phishing/Suspected domains. The submission set should include complete details of identified Phishing/Suspected domains such as detected phishing / suspected domain name, target organisation, screenshot, date and time of detection, domain registration details, hosting provider details, source of detection, execution log file, date of post (in case the phishing domain is captured through social media post) and remarks (if any). Along with the submision set, the solution and all its associated files need to be zipped (PS-02_<Application ID>_submission.zip) by the participants and submitted on the portal latest by 23:59 hours on 31st Oct 2025for evaluation. Participants will be shortlisted based on evaluation of their submitted results. Hence, it is mandatory for participants to timely submit their results. The detailed guidelines to generate the PS-02_<Application ID>_submission.zip file is mentioned at **Annexure B**.

4.2.2. **Online Solution Evaluation during Stage-1:** The evaluation of the participants in the stage-1 will be carried out on the results submitted by them as **PS-02_<Application ID>_submission.zip**. The top 15-20 participants will be selected based on the ranking on the parameters mentioned below. These numbers (15-20) may vary based on the overall performance at the discretion of the jury for this problem statement.:

STAGE 1: Total score 100		
S. No	**Name of the evaluation parameter**	**Weightage**
1	Number of Phishing Domains / URLs Detected (True Positive)	75 %
2	False Positive	25 %

4.2.3. **Solution Evaluation for shortlisted participants at the end of Stage-1:** The 15-20 selected participants will have to demonstrate their solution at FITT, IIT Delhi infrastructure on completion of Stage-1 for evaluation to select the winners of stage -1 in Nov 2025 with **PS-02_hold-out**

set. The dates for the same will be communicated to the shortlisted participants. Scores will be computed based on the evaluation metrices as mentioned below:

STAGE 1: Evaluation for Shortlisted Participants Total score 100		
S. No	**Name of the evaluation parameter**	**Weightage**
1	Number of Phishing Domains / URLs Detected (True Positive)	55%
2	False Positive	15 %
3	Approach methodology used for detection, scalability of the solution, resources used for detection.	20 %
4	Team capability to implement solution	10 %

4.2.4. If any unfair means/practices are found used by participant team, they will be disqualified.

4.2.5. Participants will be allotted slots in which they need to run their solution on reference data provided by the organizers on given resources with following tentative specifications: -

- OS – Ubuntu 24.04 LTS
- CPU – 48+ core
- RAM – 256+ GB
- Storage – 500GB

4.2.6. **Solution Demo Duration: 05 days* for each selected participant.**

***** *Subject to change based upon the feedback.*

4.2.7. Based on the results from solution demonstration and presentation, final scores will be computed based on Evaluation Metrics as mentioned at para 4.2.3 above.

4.2.8. At most, top 6 teams will be selected based on final score for **Stage - I: Evaluation for Shortlisted Participants**. These teams will be required to submit their dockerised solution with the organiser.

4.3. Datasets for Stage II:

4.3.1. **Training Dataset:** Folder "PS02_Training_set.zip" contains file having number of phishing and suspected domains corresponding to 30 identified CSEs for the solution development. It will be released at T0 of Stage 2 i.e., 16 Dec 2025. The folder will also have some sample screenshots/images of corresponding phishing pages of these CSEs.

4.3.2. **Mock Dataset:** Folder "PS02_Mock_set.zip" to contain both Phishing/Suspected URLs from CSEs. This data set will be kept updated regularly by NCIIPC, which the start-up teams/ Student groups can use to self-

evaluate their solution and the feedback to improve their solution. This update will commence from 16 Dec 2025 till 10 April 2026 as and when NCIIPC comes to know the Phishing/Suspected domains/URLs corresponding to the 30 identified CSEs.

4.3.3. **Hold-out dataset:** This set (PS-02_hold-out set_Stage2.zip) will be made available during evaluation post 11 April 2026. PS-02_hold-out set_Stage2.zip will have two sub parts. First part "PS-02_hold-out set1_Stage2" will have domains of 30 CSEs and second part "PS-02_hold-out set2_Stage2" will have a number of newly created domain names.

4.4. Evaluation for Stage-II: Stage II participants will have to upload their solution at FITT, IIT Delhi infrastructure before 23:59 Hrs on 10 April 2026.

4.5. Stage II participants will have to demonstrate their solution at FITT, IIT Delhi infrastructure after 10 April 2026 with **PS-02_hold-out set_Stage2.** The dates for the same will be communicated to the participants. ~~The winners will be decided based on above mentioned evaluation for which scores will be given based on the evaluation metrices mentioned below~~: Scores will be computed based on the evaluation metrices as mentioned below:

STAGE 2 (**Total score 100**)		
S. No	**Name of the evaluation parameter**	**Weightage**
1	Number of Phishing Domains / URLs Detected (True Positive)	45 %
2	False Positive	15 %
3	Approach methodology used for detection, scalability of the solution, resources used for detection, number of features used for identification of phishing / suspected domains and number of sources (DNS, tunnelling service, social media etc.)	20 %
4	Capability to Detect / Monitor Suspected Domain	10 %
5	Time taken for generating the Alert	10 %

4.5.1. Solution Demo Duration: 02 weeks * for each participant.

***** *Subject to change based upon the feedback.*

4.5.2. At most Top 3 teams will be selected based on final score of **Stage-II Evaluation**. These teams will be required to submit their dockerised solution with the organiser.

4.6. Datasets for Stage III:

4.6.1. **Training Dataset:** Folder "PS02_Training_set.zip" contains file having number of phishing and suspected domains corresponding to 50 CSEs for the solution development. It will be released at T0 of Stage III i.e., 01 May 2026. The folder will also have some sample screenshots/images of corresponding phishing pages of these CSEs.

4.6.2. **Mock Dataset:** Folder "PS02_Mock_set.zip" to contain both Phishing/Suspected URLs from CSEs. This data set will be kept updated regularly by NCIIPC, which the start-up teams/ Student groups can use to self-evaluate their solution and the feedback to improve their solution. This update will commence from 01 May 2026 till 25 Sep 2026 as and when NCIIPC comes to know the Phishing/Suspected domains/URLs corresponding to the 50 identified CSEs.

4.6.3. **Hold-out dataset:** This set (PS-02_hold-out set_Stage3.zip) will be made available during evaluation post 26 Sept 2026. PS-02_hold-out set_Stage3.zip will have two sub parts. First part "PS-02_hold-out set1_Stage3" will have domains of 50 CSEs and second part "PS-02_hold-out set2_Stage3" will have a number of newly created domain names.

4.7. Evaluation for Stage-III: Stage III participants will have to upload their solution at FITT, IIT Delhi infrastructure before 23:59 Hrs on 25 Sept 2026.

4.8. Stage III participants will have to demonstrate their solution at FITT, IIT Delhi infrastructure after 26 Sep 2026 ~~during 26 Sept 2026 till 10 Oct 2026~~ with **PS-02_hold-out set_Stage3.** The dates for the same will be communicated to the participants.Scores will be computed based on the evaluation metrices as mentioned below

STAGE 3 (Total score 100)		
S. No	**Name of the evaluation parameter**	**Weightage**
1	Number of Phishing Domains / URLs Detected (True Positive)	45 %
2	IDN domain detected (True positive)	05 %
3	False Positive	10 %
4	Approach methodology used for detection, scalability of the solution, resources used for detection, number	20 %

	of features used for identification of phishing / suspected domains and number of sources (DNS, tunnelling service, social media etc.)	
5	Capability to Detect / Monitor Suspected Domain	10 %
6	Time taken for generating the Alert	10 %

4.8.1. Solution Demo Duration: 02 weeks * for each selected participant.

***** *Subject to change based upon the feedback.*

4.8.2. Winner will be selected based on final score of Stage-III Evaluation. The winner team will be required to submit its dockerised solution with the organiser.

5. Q&A sessions with Mentors / Experts

For Stage-1 the organiser plans to meet participants online via online meet or email to resolve their doubts, if any. This provision will be made active from 15th Aug 2025 and details regarding interaction will be shared on this website. Kindly keep viewing this website regularly for updates on this.

Annexure A

URL-Based Features:

- URL Length
- Number of Dots in URL
- Having Repeated Digits in URL
- Number of Special Characters in URL
- Number of Hyphens in URL
- Number of Slashes in URL
- Number of Underscores in URL
- Number of Question Marks in URL
- Number of Equal Signs in URL
- Number of Dollar Signs in URL
- Number of Exclamation Marks in URL
- Number of Hashtags in URL
- Number of Percent Signs in URL
- Domain Length
- Number of Hyphens in Domain
- Having Special Characters in Domain
- Number of Special Characters in Domain

Subdomain-Based Features:

- Number of Subdomains
- Average Subdomain Length
- Subdomain Complexity (e.g., length, characters)
- Having Hyphen in Subdomain
- Having Repeated Digits in Subdomain

Path-Based Features:

- Path Length
- Having a Query in Path
- Having Fragment in Path
- Having Anchor in URL

Favicon Features:

- Favicon Presence (True/False)
- Favicon Hash (comparison with known legitimate)
- Favicon Color Scheme Similarity (using color analysis algorithms)

Image-Based Features:

- Number of Images on the Page
- Image Quality (e.g., resolution, compression)
- OCR Extracted Text (analyzing images with embedded text)
- Image Metadata (capturing EXIF data)
- Visual Design Similarity to Known Websites

Entropy and Miscellaneous:

- Entropy of URL
- Entropy of Domain
- SSL/HTTPS Presence
- Domain Registration Data (e.g., newly registered domain)

Annexure B

Guide to Output Submission Format and File/Folder Naming Structure for PS-02 Developers

1. Introduction

a. Purpose: This document provides a standard format and naming structure for PS-02 developers to ensure consistency and ease of access and review of results for the organiser.

b. Scope: This guide applies to the output report, evidences and documentation formats.

2. Each team must create a folder named exactly as <Problem_Statement_Number>_<Application ID>_Submission. This folder will contain all results of final submission materials. Eg: PS-02_AIGR-123456_Submission.

This folder to have the following files and folders:

- <Problem_Statement_Number>_<Application_ID>_Submission_Set.xlsx.
- <Problem_Statement_Number>_<Application_ID>_Evidences
- <Problem_Statement_Number>_<Application_ID>_Documentation_folder

3. About the file named **<Problem_Statement_Number>_<Application_ID>_Submission_Set.xlsx:**

Inside the main folder, include an Excel file named <Problem_Statement_Number>_<Application_ID>_Submission_Set.xlsx. (Eg: *PS-02_AIGR-123456_Result.xlsx).* This Excel file must list all the phishing and suspected domains, using the following specified column naming format:

a. Application_ID

b. Source of detection

c. Identified Phishing/Suspected Domain Name

d. Corresponding CSE Domain Name

e. Critical Sector Entity Name

f. Phishing/Suspected Domains (i.e. Class Label)

g. Domain Registration Date

h. Registrar Name

i. Registrant Name or Registrant Organisation

j. Registrant Country

k. Name Servers

l. Hosting IP

m. Hosting ISP

n. Hosting Country

o. DNS Records (if any)

p. Evidence file name

q. Date of detection (DD-MM-YYYY)

r. Time of detection (HH-MM-SS)

s. Date of Post (If detection is from Source: social media)

t. Remarks (If any)

4. About the folder named **<Problem_Statement_Number>_<Application_ID>_Evidences:**

a. Create a subfolder inside the main folder with name <Problem_Statement_Number>_<Application_ID>_Evidences (*E.g. PS-02_AIGR-123456_Evidences*).

b. This folder should contain all your supporting evidence (i.e. screenshots of phishing pages detected; one (01) screen shot of each phishing domain) in .pdf format. Each of these .pdf file must follow the following naming format: <Target_org_name>_<Up to Two-level subdomain_Name of the detected phishing domain>_<S.No>.pdf.

c. E.g., If you detect 03 phishing domains of SBI and 01 phishing domain of PNB during the mentioned period (i. the .pdf file will be named as below:

S. No	Identified Domain Name	Evidence file name (*this file to have snapshot of the phishing page)*
1	sbi123.co.in	SBI_sbi123.co.in_1.pdf
2	xyz.abc.sbi.123.com	SBI_sbi.123.com_2.pdf
3	123.abc.123.com/login/sbi	SBI_abc.123.com_3.pdf
4	pnbonline.banking.com	PNB_ pnbonline.banking.com_4.pdf

d. The evidence file names you refer in your excel file under the 'Evidences file name' column must exactly match the filenames in the

'<Problem_Statement_Number>_<Application_ID>_Evidences' folder. Any mismatch will cause your shared evidence(s) to be skipped during evaluation.

5. About the folder named **<Problem_Statement_Number>_<Application_ID>_ Documentation _folder:**

a. Create a folder named <Problem_Statement_Number>_<Application_ID>_ Documentation _folder inside your main folder. This folder should contain steps used to produce your results and also a well-written PDF document that explains your solution thoroughly. There is no restriction on how you organize the Documentation folder internally, but it should reflect a working state or final version of your solution. Also a README file is encouraged for clarity.

b. The PDF document that explains your solution thoroughly must be named <Problem_Statement_Number>_<Application_ID>_Report.pdf (E.g. *PS-02_AIGR-123456_Report.pdf*) and written using Arial font, size 12, with the text fully justified.

c. The PDF document should include clear flowcharts or architecture diagrams wherever applicable. The PDF must be structured using the following sections, in order:

   i. Participant (Start-ups/Student group) details and Skill sets
   ii. Detailed Problem Statement – clearly describe what you were solving.
   iii. Proposed Approach and Scope – explain your detection logic, research or algorithms.
   iv. Architecture – provide diagrams and a description of your system or pipeline.
   v. Implementation Details – describe the technologies, tools, datasets and Features (Indicative list as Annexure A) used for detection.
   vi. Scalability of the solution
   vii. Resources used for detection.
   viii. How to Setup and Run the soultion – instructions for installing and executing your solution on the platform.
   ix. Results – showcase the output, domain examples, metrics, etc.
   x. Conclusion – your findings, limitations and future improvements.
   xi. References – any tools, research papers or datasets cited during the solution implementation.

6. Once your folder is ready with proper naming structure mentioned above, compress (zip) your main folder. The final zipped file should look like: <Problem_Statement_Number>_<Application ID>_Submission.zip. (E.g.: *PS-02_AIGR-123456_ Submission.zip*)

7. Submit your zipped folder to NCIIPC AI Grand Challenge portal. Only one submission per team is allowed.

8. Ensure your submission is made before the deadline. Late submissions may not be evaluated.

9. Folder Structure:

<Problem_Statement_Number>_<Application_ID>_Submission/

├─── <Problem_Statement_Number>_<Application_ID>_Submission_Set.xlsx

├─── <Problem_Statement_Number>_<Application_ID>_Evidences/

│ ├─── <Target_org_name>_<Up_to_Two-level_subdomain_Name>_<S.No>.pdf

│ ├─── <Target_org_name>_<Up_to_Two-level_subdomain_Name>_<S.No>.pdf

│ └─── ...

├─── <Problem_Statement_Number>_<Application_ID>_Documentation_folder/

│ └─── <Problem_Statement_Number>_<Application_ID>_Report.pdf

10. Example of a Folder Structure:

As we are dealing with Problem Statement 02 and example Application ID *AIGR-123456*. Here is how the folder structure would look:

PS-02_AIGR-123456_Submission/

├─── PS-02_AIGR-123456_Submission_Set.xlsx

├─── PS-02_AIGR-123456_Evidences/

│ ├─── SBI_sbi123.co.in_1.pdf

│ ├─── SBI_sbi.123.com_2.pdf

│ ├─── SBI_abc.123.com_3.pdf

│ └─── PNB_ pnbonline.banking.com_4.pdf

├─── PS-02_AIGR-123456_Documentation_folder/

│ └─── PS-02_AIGR-123456_Report.pdf

Note: Submissions that do not strictly follow the prescribed folder structure, naming conventions and file format requirements, may be disqualified from evaluation.