**MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION, MUMBAI**

**GOVERNMENT POLYTECHNIC KARAD**

**THIRD YEAR DIPLOMA COMPUTER ENGINEERING (I-SCHEME)**

**PART [B]**

**MICRO-PROJECT REPORT**

# "MITIGATING PHISHING ATTACKS USING MACHINE LEARNING TECHNIQUES"

**UNDER THE SUBJECT**

**Emerging Trends in Computer and Information Technology (22618)**

**SUBMITTED BY**


| Sr.no | Roll No | Enrollment No | Name of Team Member |
|---|---|---|---|
| 1. | 2251 | 2100100053 | Pratik Pramod Shejwal |
| 2. | 2254 | 2100100056 | Shravani Bharat Mahajan |
| 3. | 2260 | 2100100063 | Riya Sunil Kharade |


**UNDER THE GUIDANCE**

**Mrs. M.A. Birnale**


**(DEPARTMENT OF COMPUTER ENGINEERING)**


**2023-24**

# Certificate of completion

## Of Micro-project Assessment at the end of Semester

This is to certify that,

| Sr.no | Roll No | Enrollment No | Name of Team Member |
|---|---|---|---|
| 1. | 2251 | 2100100053 | Pratik Pramod Shejwal |
| 2. | 2254 | 2100100056 | Shravani Bharat Mahajan |
| 3. | 2260 | 2100100063 | Riya Sunil Kharade |

Has successfully completed "MITIGATING PHISHING ATTACKS USING MACHINE LEARNING TECHNIQUES" Micro-project of the Sixth semester Diploma in Computer Engineering of subject Emerging Trends in Computer and Information Technology (22618) from Government Polytechnic Karad. Institute with Institute code (0010).

| **Mrs. M.A.Birnale** | **Prof. S. B. Patil** | **Dr. K. M. Bagwan** |
|---|---|---|
| (Project Guide) | (Head of the department.) | (Head of Institute) |

**Seal of the institute**

# ACKNOWLEDGEMENT

We take this opportunity to thank all those who have directly and indirectly inspired, directed and assisted us towards successfully completion of this project report.

We express our sincere thanks to Dr. K. M. Bagwan Principal of Government Polytechnic, Karad and the Head of Department Prof. Patil S.B, for having us allowed to submit this report as a part of our academic learning.

We express our sincere thanks to Mrs. M.A. Birnale Lecturer in Computer Engineering, Govt. Polytechnic, Karad for encouragement throughout the project report and guideline in designing and working out this project. We are also grateful to team of project.

Place: Government Polytechnic Karad

Date: 30-03-2024

**Yours Sincerely,**

2251-Pratik Pramod Shejwal

2254-Shravani Bharat Mahajan

2260-Riya Sunil Kharade

## ➢ RATIONALE

Phishing tricks online aim to deceive people into sharing private information, and current detection methods often lag behind hackers' innovations. Machine learning offers a solution by training computers to swiftly identify these traps, outsmarting cyber crooks. With machine learning, we stay proactive against threats, safeguarding personal data from falling into the wrong hands. It's like having a digital watchdog, keeping us one step ahead in the cybersecurity game. This approach strengthens our defenses, ensuring our online safety and peace of mind.

## ➢ AIM AND BENEFITS

**◉ AIM:**

1) **Spotting Phishing Tricks:**
   Teach computers to quickly identify phishing emails by analyzing sender, content, and language cues.

2) **Quick Protection:**
   Implement real-time phishing attack detection systems using machine learning for immediate response.

**◉ BENEFITS:**

1) **Enhanced Security:**
   Machine learning improves email security by swiftly identifying and blocking phishing attempts, protecting personal information.

2) **Cost Savings:**
   Early detection of phishing attacks reduces financial losses and expenses associated with cybersecurity breaches, ensuring financial stability.

## ➢ COURSE OUTCOMES ACHIEVED

CO A] Describe Artificial Intelligence, Machine learning and deep learning.

CO F] Describe Network, Operating System and applications vulnerabilities.

## ➢ LITERATIVE REVIEW

1. We Referred Book “A MACHINE LEARNING APPROACH TO PHISHING DETECTION AND DEFENSE ” by Oluwatobi Ayodejo Akanbi and his team.
2. We Referred Following Link:
    a) https://en.wikipedia.org/wiki/Machine_learning
    b) https://www.geeksforgeeks.org/machine-learning/
    c) https://www.phishprotection.com/phishing-awareness/machine-learning-helps-fighting-phishing-attacks

## ➢ ACTUAL METHODOLOGY FOLLOWED

1. Discussion about given topic.
2. Selection of good leader and distribution of responsibilities.
3. Collection of information using different resources, Analysis of given information.
4. Presentation of given report.
5. Completion and submission of given tasks.

## ➢ ACTUAL RESOURCES USED

| No | Name of the Resource | Specifications | Quantity | Remark |
|---|---|---|---|---|
| 1 | Computer System | At least 4GB RAM, i5 Processor | 1 | Required |
| 2 | Software | Microsoft word | 1 | Required |

## ➢ OUTPUT OF MICROPROJECT:

In our microproject titled "Mitigating Phishing Attacks Using Machine Learning Techniques," we've explained simple concepts about machine learning and phishing. We talked about how phishing tricks people online and why it's a big problem. We described how phishing attacks happen and the harm they cause to people and companies. We stressed why it's crucial to stop phishing to protect online safety. Additionally, we discussed how machine learning methods can help fight against phishing, making it easier to understand and use in real situations.

## ➢ SKILLS DEVELOPED OF THIS MICRO-PROJECT

1. **Cybersecurity Awareness**:

   understand how machine learning can help in fighting against them.

2. **Problem-solving and Critical Thinking:**

   Learners will improve their ability to solve real-world problems related to phishing by critically analyzing detection methods.

3. **Machine Learning Fundamentals:**

   Participants will gain a strong understanding of machine learning algorithms.

4. **Project Management:**

   You'll gain experience in project planning, execution, testing, data collection etc.

5. **Communication Skill:**

   ability to convey information clearly and effectively to other.

## ➢ APPLICATIONS OF MICRO-PROJECT

1. **Social Media Monitoring:**

   Utilize machine learning to scan social media platforms for phishing scams and malicious content.

2. **Website URL Analysis:**

   Teach a machine learning model to analyze website URLs for signs of phishing.

3. **User Behaviour Analysis:**

   Train a model to analyze user behaviour patterns, such as clicking on links or downloading attachments.

4. **Endpoint Security Solutions:**

   Integrate machine learning algorithms into endpoint security solutions to protect devices from phishing threats.