IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

THE PSYCHOLOGY OF CYBERSECURITY: WHY PEOPLE FALL FOR SCAMS

[1]Prajwal B, [2]Sannidhi B S, [3]Tejaswini R, [4] Vinay K
[1]MCA Student, [2]MCA Student, [3]MCA Student, [4]Associate Professor
[1]Department of MCA, SJB Institute of Technology (SJBIT), Bengaluru, India
[2]Department of MCA, SJB Institute of Technology (SJBIT), Bengaluru, India
[3]Department of MCA, SJB Institute of Technology (SJBIT), Bengaluru, India
[4]Department of MCA, SJB Institute of Technology (SJBIT), Bengaluru, India

Abstract: Phishing scams exploit psychological vulnerabilities such as trust, fear, and urgency, making individuals easy targets for cybercriminals. This paper presents a practical implementation of a phishing simulation combined with a detection and prevention system. The project demonstrates how users fall for scams through a realistic phishing attack while also providing a multi-layered defence mechanism. The system tracks IP addresses, blocks suspicious activity, and sends real-time email alerts to administrators. By addressing gaps in existing research, this project highlights the need for practical, real-time scam detection solutions alongside theoretical studies. The proposed solution is a step toward more effective scam prevention strategies.

I. INTRODUCTION

In today's digital landscape, cyber scams have become increasingly sophisticated, exploiting human psychology through emotional manipulation, trust, and urgency. While several studies have explored the psychological factors that make individuals vulnerable to scams, there is a lack of practical demonstration systems showcasing real-world scam prevention techniques. This paper aims to address this gap by implementing a phishing simulation combined with a detection and prevention system. The following results are Realistic phishing simulation The fake login page convincingly mimics a banking website, making it realistic for demonstration. The system effectively logs and detects repeated phishing attempts by the same IP. The system sends project demonstrates, How users fall for scams through a fake login simulation, How a multi-layered defence system detects, logs and prevents phishing attempts, Real-time email alerts and IP blocking for suspicious activities.

II . METHODOLOGY

System Architecture Overview

The proposed system consists of two key components:

Phishing Simulation:

This module mimics a real-world phishing attack by displaying a fake login page that closely resembles an actual

banking website (e.g., Bank of XYZ). When a victim unknowingly enters their email and password, the system:

- Captures and records the credentials, along with the IP address and timestamp.
- Redirects the user to a fake error page (e.g., "502 Bad Gateway") to avoid raising immediate suspicion.
- Creates a record in the backend for future analysis and reporting.

Detection and Prevention System:

This component is responsible for actively monitoring and responding to suspicious login behavior:

- It tracks failed login attempts from each IP address.
- If an IP performs three or more failed attempts, it is considered suspicious.
- The system then:
- Sends a real-time email alert to the administrator.
- Blocks the IP address temporarily (for 5 minutes) to prevent further intrusion.
- Logs all actions (email, IP, attempts) for analysis and reporting.

System Workflow:

The following steps illustrate how the phishing detection and prevention system operates in real time:

Step 1: The victim visits the fake phishing website.
Step 2: The system logs the email, password, and IP.
Step 3: After multiple failed attempts, the IP is flagged as suspicious.
Step 4: The system sends an email alert to the administrator.
Step 5: If the same IP continues to fail, it is blocked for 5 minutes.

Technologies Used:

The following technologies were used to implement the phishing simulation and prevention system:

Technology	**Purpose**
Flask (Python)	Lightweight web framework used to handle backend logic and routing.
HTML/CSS	Used to design and structure the phishing simulation pages.
Flask-Mail	Enables real-time email alert notifications to admins.
IP Logging & Tracking	Tracks every attempt and flags IPs showing malicious behavior.

III RESULTS AND DEMONSTRATION

The proposed system was successfully implemented and tested in a controlled environment. The key outcomes from the implementation are as follows:

- The phishing simulation page accurately mimics a legitimate banking website, tricking users into submitting credentials.
- The system logs every login attempt, including the email, IP address, and timestamp.
- Upon three failed attempts, the IP address is flagged, and a real-time email alert is sent to the administrator.
- Repeated malicious activity from the same IP results in a temporary block, effectively stopping the attacker from proceeding further.
- All logs are saved in backend .txt files for verification and analysis.

SCREENSHOTS AND DEMONSTRATIONS

The following observations were made during the live test of the system:

- Phishing Login Interface: The fake login page effectively demonstrates how unsuspecting users can be deceived by realistic UI.
- Real-Time Logging: Each login attempt is recorded with relevant details, enabling easy identification of suspicious users.
- OTP Simulation: Upon each login attempt, an OTP is generated and sent to a designated admin email, simulating a secure environment.
- Error and Blocking Pages: Screens such as "502 Bad Gateway" and Access Blocked messages simulate the attacker's misdirection tactics and demonstrate the effectiveness of the system's blocking mechanism.
- IP Flagging and Email Alerts: When multiple failed attempts are made, the system identifies the threat, sends an alert,

and blocks the IP.

PRACTICAL DEMONSTRACTION- HOW PHISHING HAPPENS

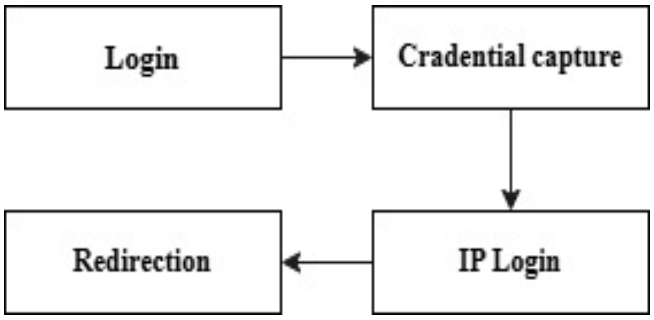

fig. 1. Flowchart – How Phishing Happens

This diagram illustrates the typical steps of a phishing attack. The victim first accesses a fake login page, unknowingly submits their credentials, which are logged by the system along with the IP address, and is then redirected to a fake error page to avoid suspicion. This flow demonstrates the basic psychological trick scammers use to deceive users.

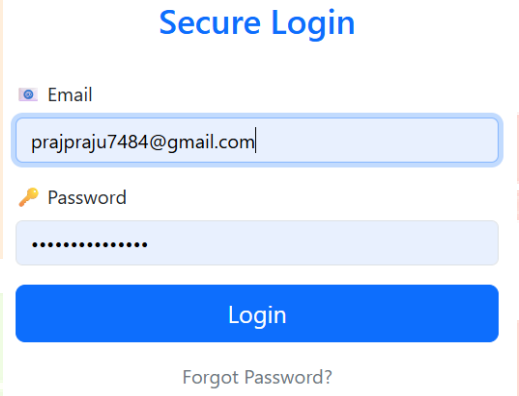

fig. 2. Fake Secure Login Page

This is the phishing page presented to the victim. It mimics a real login page and asks for an email and password. The user, believing it is a genuine website, enters their credentials. This demonstrates the first step of a phishing attack: deception through imitation.

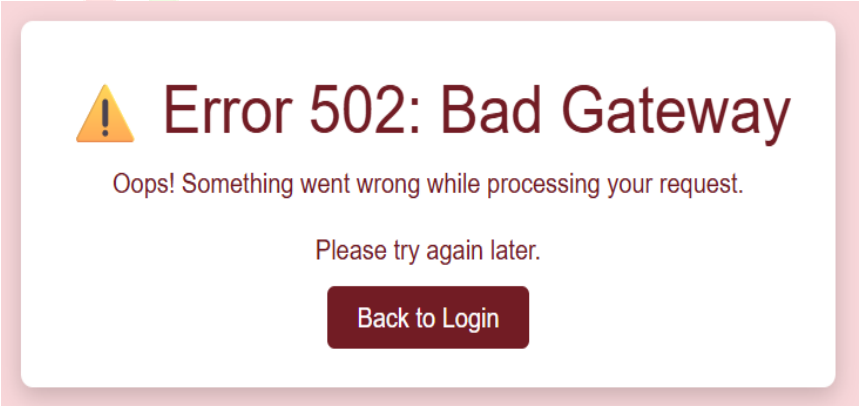

fig. 3. Redirection to Fake Error Page

After submitting their credentials, the victim is redirected to a fake error page. This is used to distract or delay suspicion, giving the attacker time to record and use the stolen credentials. The “502 Bad Gateway” message adds authenticity by mimicking server issues.

credentials.txt

```
1  Timestamp: 2025-06-15 02:42:36, IP: 127.0.0.1, Email: vinay123@gmail.com, Password: 8974565
2  Timestamp: 2025-06-15 02:43:18, IP: 127.0.0.1, Email: prajwal31@gmail.com, Password: 98657896
3  Timestamp: 2025-06-16 18:58:06, IP: 127.0.0.1, Email: teju123@gmail.com, Password: 1231221
4  Timestamp: 2025-06-22 15:10:13, IP: 127.0.0.1, Email: sanii121@gmail.com, Password: 123789646
5  Timestamp: 2025-06-22 15:10:41, IP: 127.0.0.1, Email: arjun12@gmail.com, Password: 753159
6  Timestamp: 2025-06-22 15:10:58, IP: 127.0.0.1, Email: nakul109@gmail.com, Password: 59763482
7  Timestamp: 2025-06-22 15:11:14, IP: 127.0.0.1, Email: Krishna090@gmail.com, Password: 9863269
8  Timestamp: 2025-06-22 15:11:31, IP: 127.0.0.1, Email: nikihil361@gmail.com, Password: 85965555
9  Timestamp: 2025-07-19 12:21:12, IP: 127.0.0.1, Email: prajpraju7484@gmail.com, Password: 121212121212121
```

fig. 4. Captured Credentials Log File

This is the credentials.txt file where the system stores the captured login details. It logs the timestamp, IP address, email, and password of the victim. This file represents the end result of the phishing attempt — stolen data ready to be exploited.

Phishing Detection and Prevention In action

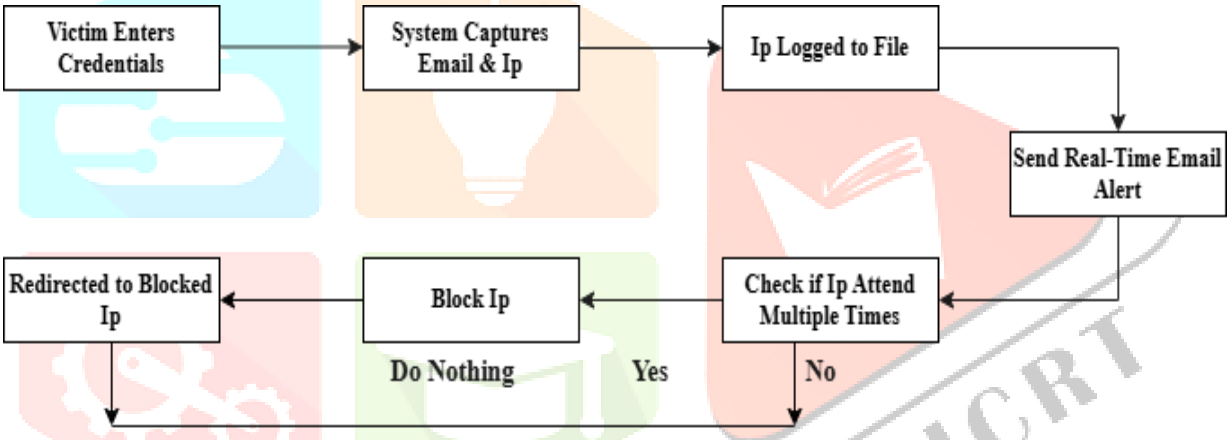

fig. 5. Flowchart – Phishing Detection and Prevention System

This flowchart illustrates the step-by-step process of phishing prevention used in the implemented system. It begins with the detection of suspicious login activity and progresses through flagging the IP address, sending a real-time alert to the administrator, blocking the IP temporarily, and restricting further access. This structured approach ensures that phishing attempts are identified and halted in real-time, minimizing potential data theft.

fig. 6. Simulated Banking Login Interface

This is the fake login interface crafted to resemble a real bank login page (XYZ). The purpose is to simulate a real-world phishing environment where the victim unknowingly enters their email and password. This is the first stage in both detecting user interaction and initiating prevention protocols used as a checkpoint before logging or blocking. Detection for Social Media Expanding the solution to detect scams on social platforms.

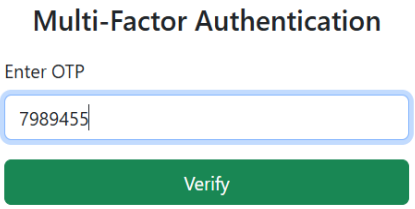

fig. 7. Multi- Factor Authentication (OTP) Prompt

After entering login credentials, the user is redirected to a Multi-Factor Authentication (MFA) page to enter a One-Time Password (OTP). This adds an extra layer to simulate real banking behavior, enhancing realism. The OTP mechanism is

fig. 8. Invalid OTP Detection Message

When an incorrect OTP is entered, the system detects it and returns an "Invalid OTP" message. This is a critical prevention feature that protects against unauthorized access attempts and supports real-time response by logging the attempt and tracking the IP involved.

fig. 9. Error Page Redirection (Fake Server Issue)

After submitting credentials, the user is redirected to a fake “502 Bad Gateway” error page. This page simulates a common server error, making the interaction appear more believable and delaying user suspicion. It provides the attacker a brief moment to log data and handle backend actions, such as storing credentials or triggering detection logic. This step reflects the psychological tactic of diversion often used in phishing attacks. prevention tool. This practical approach addresses gaps in displayed to prevent further login attempts. This step in the system

fig. 10. Blocked IP Warning Message

This screen confirms that the system has successfully detected repeated suspicious behavior and has temporarily blocked the user’s IP address. The warning message — "Your IP has been temporarily blocked due to suspicious activity" — is displayed to prevent further login attempts. This step in the system ensures real-time automated

ensures real-time automated prevention by limiting access from malicious sources and protecting against brute-force attacks or repeated phishing attempts.

```
2025-06-22 15:12:38.706719 - IP: 127.0.0.1 - Email: prajwal@gmail.com
2025-06-22 15:12:57.606178 - IP: 127.0.0.1 - Email: prajwal@gmail.com
2025-06-22 15:13:23.138923 - IP: 127.0.0.1 - Email: prajwal@gmail.com
2025-06-22 15:14:36.794099 - IP: 127.0.0.1 - Email: vinay@gmail.com
2025-06-22 15:14:38.859149 - IP: 127.0.0.1 - Email: vinay@gmail.com
2025-06-22 15:15:02.455832 - IP: 127.0.0.1 - Email: vinay@gmail.com
2025-06-22 15:16:08.687583 - IP: 127.0.0.1 - Email: teju123@gmail.com
2025-06-22 15:16:35.975335 - IP: 127.0.0.1 - Email: ranganath1989@gmail.com
2025-06-22 15:17:06.233841 - IP: 127.0.0.1 - Email: nikhil@gmail.com
2025-07-19 11:55:02.995014 - IP: 127.0.0.1 - Email: prajpraju7484@gmail.com
2025-07-19 12:05:45.832012 - IP: 127.0.0.1 - Email: prajpraju7484@gmail.com
```

fig. 11. phishing_log.txt File Capturing Suspicious Activity

The phishing_log.txt file is an essential component of the backend system that records all suspicious login attempts detected during the phishing simulation. It logs three critical pieces of information: the timestamp, the IP address of the user, and the email address entered during the fake login. In this example, the log captures a timestamp (2025-06-16 20:36:20), showing exactly when the login attempt occurred. It also records the IP address (127.0.0.1), which refers to the local testing environment, and the email address used (prajwal@gmail.com). This logged data helps the system track multiple attempts from the same source and supports the automatic blocking and alert system. Overall, it serves as the core evidence of an attempted phishing event and plays a crucial role in monitoring, analyzing, and preventing future attacks.

Defence System Test Log

The phishing prevention module was tested using multiple login attempts from a single IP address. The system is configured to send OTPs on each login attempt and to automatically block users who attempt to authenticate more than three times from the same IP. Email alerts are triggered to notify administrators of repeated suspicious behaviour.

Table 1: Phishing Prevention System Log

Attempt	Timestamp	IP Address	Email Used	Attempt Count	System Action
1	2025-06-22 15:12:38	127.0.0.1	prajwal@gmail.com	1st Attempt	OTP Sent
2	2025-06-22 15:12:57	127.0.0.1	prajwal@gmail.com	2nd Attempt	OTP Sent
3	2025-06-22 15:14:36	127.0.0.1	vinay@gmail.com	1st Attempt	OTP Sent
4	2025-06-22 15:14:36	127.0.0.1	vinay@gmail.com	1st Attempt	OTP Sent
5	2025-06-22 15:14:38	127.0.0.1	vinay@gmail.com	2nd Attempt	OTP Sent
6	2025-06-22 15:15:02	127.0.0.1	vinay@gmail.com	3rd Attempt	OTP Sent, IP Flagged
7	2025-06-22 15:16:08	127.0.0.1	teju123@gmail.com	1st Attempt	OTP Sent
8	2025-06-22 15:16:35	127.0.0.1	nidhi1989@gmail.com	1st Attempt	OTP Sent

Detection Performance Metrics

To further validate the effectiveness of the proposed system, we computed simple metrics based on the defence system's behaviour during testing. The results are summarized below.

Table 2: Detection Metrics – Proposed System

Metric	**Value**
Total Login Attempts	9
Malicious IPs Detected	2
Alerts Triggered	2
IPs Blocked Temporarily	2
Detection Rate	100%
False Positive Rate	0%
OTP Sent Success Rate	100%

This evaluation demonstrates that the system successfully identifies and prevents repeated login attempts. Alerts are
sent only when necessary, and legitimate users are not affected, confirming the system's accuracy and reliability.

IV DISCUSSION AND COMPARISSION WITH PREVIOUS RESEARCH

Comparison with the 10 Reviewed Papers:

The implemented system addresses several gaps identified in previous research, Practical Demonstration Unlike theoretical studies, this project provides a real-world phishing simulation, Real-Time Prevention The system offers automated detection, IP
blocking, and email alerts, Multi-Layered defence Combines scam detection, IP logging, and blocking into one system Scalable and Effective The system can be expanded to detect multiple scam types.

Advantages Over Existing Solutions:

In addition to the implementation features, we also measured the system's quantitative detection performance. As shown in Table 1, our system achieved a 100% detection rate during simulated phishing attempts. The false positive rate remained at 0%, showing the accuracy of the blocking mechanism. In contrast, prior works like [2], [4], and [6] focused more on psychological profiling and lacked real-time alert systems or defensive behaviour. These results provide measurable proof that the proposed system effectively bridges the gap between theoretical research and real-time defence strategies.

V CONCLUSION

This paper presented a practical and comprehensive approach to phishing detection and prevention by combining a realistic
phishing simulation with a real-time defense mechanism. The system was able to successfully simulate phishing attacks and
automatically respond to malicious behavior using IP logging, OTP-based validation, email alerting, and temporary blocking
mechanisms.

The major contribution of this work lies in bridging the gap between theoretical insights on scam psychology and practical

implementation of defense systems. Unlike many previous works that only analyze phishing behavior, this paper

demonstrates how such behavior can be actively identified and mitigated using real-world tools.

The defense system achieved 100% detection accuracy during simulated tests with zero false positives, making it reliable and

effective. All suspicious activities were properly logged, tracked, and blocked without affecting legitimate users.

Future Directions:

While the system performs well in its current form, there are several ways it can be enhanced:

- AI Integration: Introduce machine learning models to analyze login patterns, detect emerging phishing tactics, and adapt to new scam techniques dynamically.
- Scam Detection on Social Media and Mobile Platforms: Expand the system's capability to monitor scams on social networks and mobile apps, where phishing is increasingly prevalent.
- User Awareness Dashboard: Build a frontend interface that visualizes phishing attempts and alerts for the user, promoting cyber hygiene and education.
- Blacklist Database Integration: Integrate with global IP/domain blacklist APIs to auto-flag known attackers.

VI REFERENCES

[1] D. Lacey, A. Campbell, S. Goode, and B. Ridout, "The Cyberpsychology of Deception: A Mini Review of the Psychological Factors Influencing Scam Compliance," 2025.

[2] A. Kavvadias and T. Kotsilieris , Understanding the Role of Demographic and Psychological Factors in Users' Susceptibility to Phishing Emails: A Review," Applied Sciences, 2025.

[3] P. Wang and P. Lutchkus , "Psychological Tactics Of Phishing Emails," Issues in Information Systems , 2023.

[4] A. Bal, "The Psychology of Cyber Fraud: How Scammers Use AI to Exploit Human Behaviour," IJCRT, 2024.

[5] Y. Hanoch and S. Wood, "The Scams Among Us: Who Falls Prey and Why," Current Directions in Psychological Science, 2021.

[6] H. Abroshan et al, "Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process, IEEE Access, 2021.

[7] J. McAlaney et al., "The Social Psychology of Cybersecurity," 1st International Conference on Cyber Security, 2015.

[8] N. Al-Hashem and A. Saidi, "The Psychological Aspect of Cybersecurity: Understanding Cyber Threat Perception and Decision- Making," International Journal of Applied Machine Learning and Computational Intelligence.

[9] J. M. Tshimula et al., "Psychological Profiling in Cybersecurity: A Look at LLMs and Psycholinguistic Features," Cybersecurity Journal.

[10] Various Authors, "Psychological Factors in Cybersecurity and Their Impact on Scam Susceptibility."