IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 27, Issue 4, Ser. 2 (July. – August. 2025), PP 17-25
www.iosrjournals.org

AI-Powered Phishing Simulation On Cloned UPI Interfaces For Financial Fraud Analysis

Sudesh Kumari[1], Sri Sindhu Mandava[2], Patel Mounika[3], Vuppala Bhargavi[4], Voore Manuchandana[5], Padigela Sujana[6], Kaachia Patel Het Kumar[7], Ananya Vasista[8]
Digital Forensics Division, Central Forensic Science Laboratory (CFSL), Hyderabad, India

Abstract:
This paper presents a practical simulation of phishing-based financial fraud designed to replicate the attack flow typically used to compromise Unified Payments Interface (UPI) users. The simulation environment was developed within the Digital Forensics Division at CFSL, Hyderabad, and models a cloned interface of the PhonePe application to demonstrate how cybercriminals manipulate visual trust and interface mimicry to collect sensitive user data. The system is built using Python and the Flask framework for backend handling, with HTML and CSS for replicating the user-facing interface. Key features include real-time data capture of mobile numbers and OTPs, monitored using the Watchdog library and accompanied by live desktop alerts via Plyer. The application is publicly hosted using Ngrok, enabling ethical testing of phishing delivery methods through external access. This platform was created to work safely in a controlled and secure setting, following ethical hacking practices. It's designed as a hands-on learning tool for students and professionals in cybersecurity and digital forensics. Instead of using complicated tools or advanced hacking techniques, it focuses on how simple and familiar design elements can be used to trick people. The project shows how easily trust can be misused through common interface tricks, and it reminds us how important it is to stay alert and aware, especially when it comes to avoiding phishing scams

Key Words: *Phishing simulation; digital payment security; UPI phishing; cybersecurity awareness; OTP exploitation; ethical hacking; user credential harvesting; web-based fraud; tunnel-based spoofing; interface impersonation.*

Date of Submission: 21-07-2025 Date of Acceptance: 31-07-2025

I. Introduction

Money transfers have become quicker and easier thanks to modern digital payment options. One of the biggest reasons for India's digital growth is the rise of UPI (Unified Payments Interface), which lets people send and receive money instantly. Apps like Google Pay, PhonePe, and Paytm have made digital payments popular by offering user-friendly designs, smooth shopping experiences, and attractive offers like cashback and discounts. While these changes have helped boost the digital economy, they've also brought new security risks and chances for cybercriminals to take advantage.

Since phishing is presently one of the most common and hurtful dangers, cybercriminals are focusing more on these platforms. Symantec characterizes phishing as "an endeavor to wrongfully get individual and financial data by sending a message that purports to come from a respectable and dependable organization." These messages regularly contain tricky links to imposter websites that mirror the genuine one. Individuals are tricked into giving touchy accreditations, which offenders then take. In arrange to sidestep discovery, the false site as a rule reroutes guests to the bona fide page, which lessens the perceivability of the attack. This thought centers on mirroring phishing endeavors within the UPI biological system, particularly focusing on PhonePe clients, in a secure and moral setting. By making a phishing application that mirrors PhonePe, finding security holes, and evaluating client vulnerabilities, the ponder investigates the strategies utilized by programmers. The objectives are to supply down-to-earth bits of knowledge on phishing strategies and propose effective countermeasures.

Mobile gadgets, which are fundamental for online exchanges, are particularly vulnerable to phishing attacks because of the extensive volume of personal information they store and the various services they interface with. To take advantage of these characteristics, assailants utilize complex techniques like sending fake messages and deceiving joins. These assaults highlight the need for solid security measures by posing genuine dangers, such as monetary losses and compromised data.

The outcome of the ponder is expected to upgrade the creation of secure online payment frameworks. The objective of the consideration is to form UPI-based apps more resilient to phishing assaults by identifying vulnerabilities and advertising proposals for changes to cybersecurity directions, client training, and confirmation strategies. This places too emphasis on how pivotal it is to close the hole between specialized security and client understanding in arrange to advance belief in advanced payment frameworks and ensure their reasonability in a progressively interconnected world.

Financial exchanges are presently speedier and easier due to the broad use of digital payment methods. A big part of India's digital change is the rise of UPI (Unified Payments Interface), which makes sending money quick and easy in real time. Apps like Google Pay, PhonePe, and Paytm have helped bring digital payments to the mainstream. Their popularity comes from simple, easy-to-use designs, smooth connections with online shopping, and customer-friendly features like discounts and cashback. While these tools have pushed the digital economy forward, they've also brought new risks by exposing certain security weaknesses. Since phishing is presently one of the most common and destructive dangers, cybercriminals are focusing more on these stages. Symantec characterizes phishing as "an endeavor to wrongfully get individual and financial data by sending a message that purports to come from a respectable and dependable organization." These messages regularly contain beguiling links to imposter websites that imitate the genuine one. Individuals are hoodwinked into giving touchy accreditations, which hoodlums at that point take. In arrange to evade location, the false site more often than not reroutes guests to the bona fide page, which reduces the perceivability of the attack.

II. Related Work

Phishing is still one of the most common tricks used by cybercriminals to take advantage of people's trust, especially in digital payment systems. Experts have studied phishing from different angles—how to detect it, how users react to it, and how certain designs or interfaces can be used to mislead people.

Sharma [1] studied the influence of interface design and brand trust in user adoption of UPI-based applications like Google Pay. This aligns with the design strategy used in our simulation, where a familiar interface is leveraged to create a false sense of authenticity.

Burita et al. [2] analyzed phishing email structures and emphasized the psychological manipulation involved in luring users to spoofed pages. Our work extends this by replicating the visual flow of a trusted payment app to simulate how attackers collect sensitive data.

Chaudhuri [5] introduced the concept of clone phishing, where attackers mimic entire websites or applications to harvest user credentials. Our project demonstrates this method in a controlled environment, targeting mobile users with cloned login and OTP workflows.

Amro [21] discussed the increasing risk of phishing on mobile platforms, where smaller screen sizes and limited visibility often reduce user awareness. To reflect this, our simulated phishing site is mobile-accessible, highlighting how users can be deceived even without technical compromise.

Ali and Zaharon [14] advocated for the integration of educational simulations into anti-phishing strategies. Our project supports this approach by providing an interactive, ethically built platform to raise awareness among students, researchers, and cybersecurity analysts.

These studies collectively inform the design and goals of our phishing simulation, which focuses not on detection but on understanding how real attacks unfold—thereby bridging the gap between theory and experiential learning.

III. Materials And Methods

The present project focuses on identifying and analyzing financial frauds carried out through phishing attacks that exploit legitimate-looking links or URLs. As part of a learning-focused project to spread awareness about phishing, a recreated version of the PhonePe login page was developed. The purpose of this task was to show how attackers can design fake websites to deceive users and steal their details. The demonstration was carried out in a controlled and secure setting under the close supervision of cybersecurity experts from the Digital Forensics Department at CFSL, Hyderabad. All procedures were followed responsibly, with strict attention to ethical and legal standards. This hands-on project served as a practical example of how online threats operate and highlighted the importance of being cautious while interacting with digital platforms.

Objective Of The Study

The main objective of this project is to create a credible phishing situation that closely mimics the user interface of the popular digital payment service PhonePe. This simulation aims to demonstrate how individuals can be deceived into revealing sensitive information such as phone numbers, OTPs, and UPI PINs. The project shows common phishing attacks done and various psychological techniques used by attackers to gain the credentials from the victim, and vulnerabilities that allow these threats to thrive through this analysis. Along with the technical aspect, it aims to educate users and cybersecurity enthusiasts on how effortlessly visual trust can be altered via interface imitation.

Tools And Technologies Used:

To showcase the phishing simulation, different frontend and backend technologies have been utilized, ensuring a thorough and authentic representation of a phishing process. The tools and their purposes are as follows:

- **Python** was used as the primary programming language to handle the core scripting and backend logic of the simulation.
- **Flask**, a lightweight Python web framework, was implemented to manage server-side routes and form processing.
- **HTML and CSS** were used to design the frontend interface, replicating the visual appearance of the PhonePe login and transaction pages.
- **Watchdog**, a Python library, enabled real-time monitoring of file changes, specifically for detecting new entries in the credentials log file.
- **Plyer** was integrated to provide instant desktop notifications whenever new data was captured, simulating live alerts.
- **Ngrok** was employed to generate a secure, public-facing URL, allowing external devices to access the locally hosted simulation.
- **Visual Studio Code (VS Code)** served as the development environment, offering a convenient platform for coding and debugging.
- **Google Chrome** was used as the primary browser for testing and validating the simulated phishing pages across different devices.

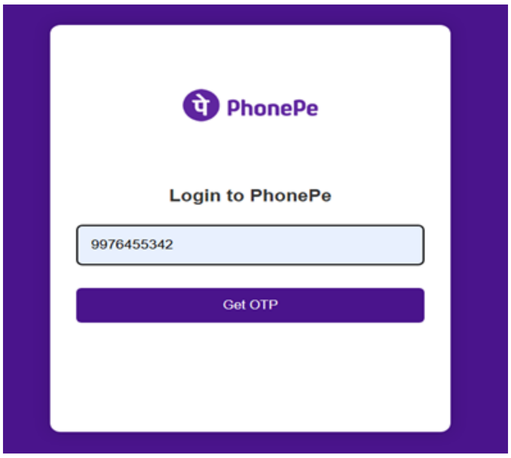
Design And Development Process

The development of the phishing simulation was carried out in well-planned steps, each designed to closely imitate the methods commonly used by cyber attackers in real-life scenarios. The primary goal was to create a fully functional mock system that educates users about the anatomy of phishing schemes by demonstrating each phase of the attack cycle. The process unfolded through the following steps:

Step 1: Simulating the Phishing Workflow

The first step in the project involved designing a responsive web interface that convincingly imitates PhonePe's login pages. The interface includes:

- **Login Page:** Users are prompted to enter their registered mobile number and a dummy password.



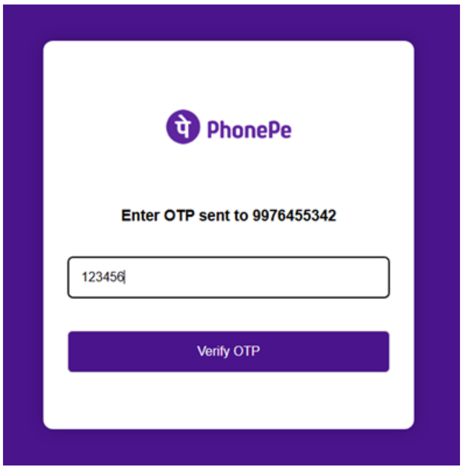
PhonePe

Login to PhonePe

9976455342

***Fig 3.1** — Screenshot of the PhonePe-style Login Page*

- **OTP Page:** Simulates the entry of a One-Time Password.

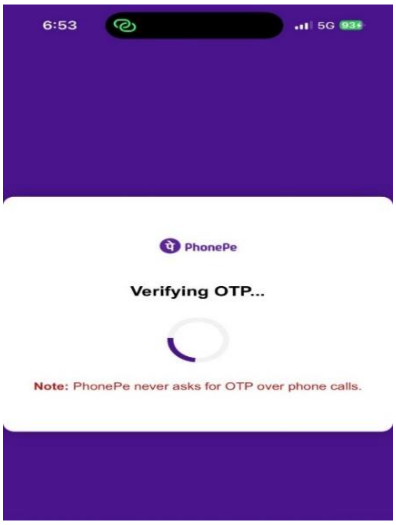


Enter OTP sent to 9976455342

123456

***Fig 3.2** — Screenshot of the OTP Entry Page*

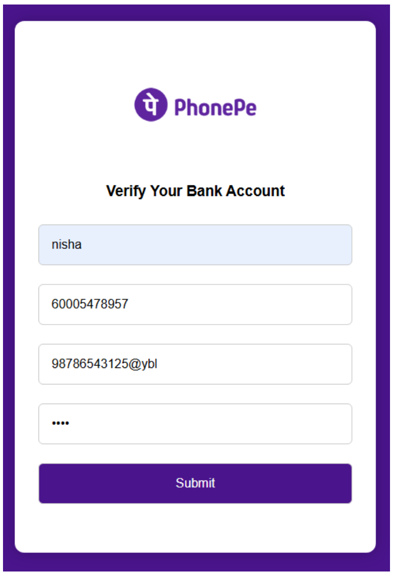
- **Account Details Page:** Mimics the final stage where UPI PINs or other credentials are entered.



Verifying OTP...

Note: PhonePe never asks for OTP over phone calls.

***Fig 3.3** — Verifying OTP*



Verify Your Bank Account

nisha

60005478957

98786543125@ybl

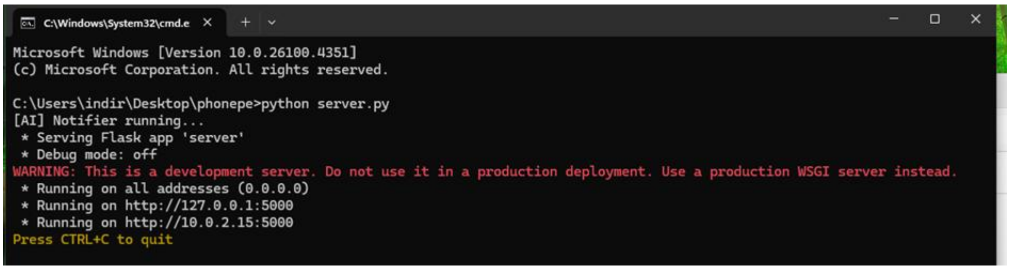
••••

***Fig 3.4** — Screenshot of the Account Details Page*

Each page was crafted using HTML and styled with CSS to provide a genuine look and feel. Flask was used to serve the pages and route users through the simulated user journey, just as an actual attacker would do in a real-world phishing setup.

Step 2: Backend Integration Using Flask

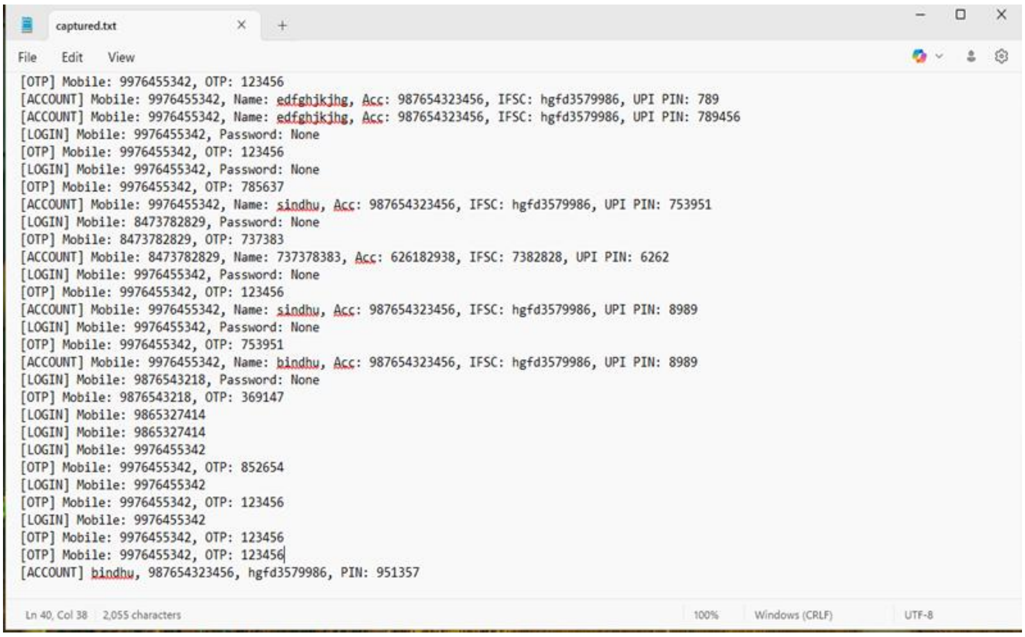
The backend of the phishing simulation was developed using the Flask web framework, which facilitated route handling for different stages of the user interaction, including /login, /otp, and /submit account. When users submitted input on the spoofed interface, the system captured and stored sensitive information such as mobile numbers, one-time passwords (OTPs), and UPI credentials in a local text file named captured.txt. As depicted in **Fig. 3.5**, the Flask development server was executed via the terminal to host the simulation locally. Subsequently, all collected data was logged and visualized in the captured.txt file, mimicking the data harvesting techniques used by threat actors, as illustrated in **Fig. 3.6**. This setup allowed ethical investigators to analyze how phishing systems record user credentials in real-world attack scenarios.



```
Microsoft Windows [Version 10.0.26100.4351]
(c) Microsoft Corporation. All rights reserved.

C:\Users\indir\Desktop\phonepe>python server.py
[AI] Notifier running...
 * Serving Flask app 'server'
 * Debug mode: off
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
 * Running on all addresses (0.0.0.0)
 * Running on http://127.0.0.1:5000
 * Running on http://10.0.2.15:5000
Press CTRL+C to quit
```

Fig 3.5 — Flask Server Running in the Terminal

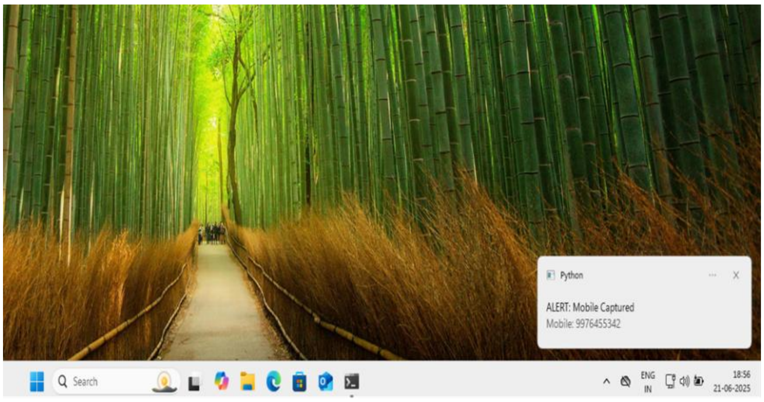


```
[OTP] Mobile: 9976455342, OTP: 123456
[ACCOUNT] Mobile: 9976455342, Name: edfghjkjhg, Acc: 987654323456, IFSC: hgfd3579986, UPI PIN: 789
[ACCOUNT] Mobile: 9976455342, Name: edfghjkjhg, Acc: 987654323456, IFSC: hgfd3579986, UPI PIN: 789456
[LOGIN] Mobile: 9976455342, Password: None
[OTP] Mobile: 9976455342, OTP: 123456
[LOGIN] Mobile: 9976455342, Password: None
[OTP] Mobile: 9976455342, OTP: 785637
[ACCOUNT] Mobile: 9976455342, Name: sindhu, Acc: 987654323456, IFSC: hgfd3579986, UPI PIN: 753951
[LOGIN] Mobile: 8473782829, Password: None
[OTP] Mobile: 8473782829, OTP: 737383
[ACCOUNT] Mobile: 8473782829, Name: 737378383, Acc: 626182938, IFSC: 7382828, UPI PIN: 6262
[LOGIN] Mobile: 9976455342, Password: None
[OTP] Mobile: 9976455342, OTP: 123456
[ACCOUNT] Mobile: 9976455342, Name: sindhu, Acc: 987654323456, IFSC: hgfd3579986, UPI PIN: 8989
[LOGIN] Mobile: 9976455342, Password: None
[OTP] Mobile: 9976455342, OTP: 753951
[ACCOUNT] Mobile: 9976455342, Name: bindhu, Acc: 987654323456, IFSC: hgfd3579986, UPI PIN: 8989
[LOGIN] Mobile: 9876543218, Password: None
[OTP] Mobile: 9876543218, OTP: 369147
[LOGIN] Mobile: 9865327414
[LOGIN] Mobile: 9865327414
[LOGIN] Mobile: 9976455342
[OTP] Mobile: 9976455342, OTP: 852654
[LOGIN] Mobile: 9976455342
[OTP] Mobile: 9976455342, OTP: 123456
[LOGIN] Mobile: 9976455342
[OTP] Mobile: 9976455342, OTP: 123456
[OTP] Mobile: 9976455342, OTP: 123456
[ACCOUNT] bindhu, 987654323456, hgfd3579986, PIN: 951357
```

Fig 3.6 — Captured.txt Log File Showing Recorded Credentials

Step 3: Real-Time Monitoring with Watchdog and Plyer

To simulate automation and mimic attacker-like behavior, the **Watchdog** library in Python was integrated to continuously monitor the **captured.txt** file for updates. Whenever a new mobile number was recorded**, Plyer** triggered a desktop notification to alert the ethical analyst in real time. This mechanism mirrors how real attackers or bots track user inputs as they interact with phishing pages. As depicted in **Fig. 3.7**, this real-time alert system not only adds practical value to the simulation but also helps users understand how quickly sensitive data can be collected and observed during a live phishing attempt.



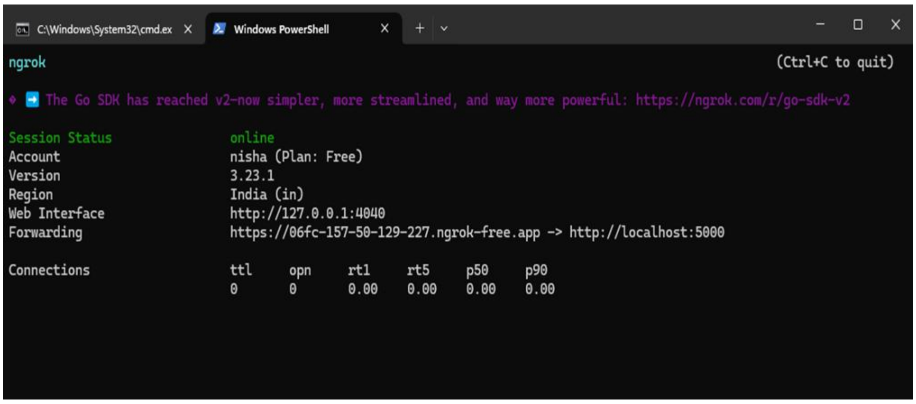
Python

ALERT: Mobile Captured
Mobile: 9976455342

Fig 3.7 — Desktop Notification Showing Captured Mobile Number

Step 4: Public Hosting Using Ngrok

To simulate the behavior of phishing attacks beyond local environments, the Flask application was made accessible over the internet using Ngrok, which established a secure HTTPS tunnel. This enabled the generation of a public-facing URL that could be accessed from various devices, including smartphones and external systems. As illustrated in **Fig. 3.8**, this configuration mirrors the distribution methods typically employed by attackers—such as SMS, email, or social media—making it possible to deliver deceptive links under the appearance of legitimate web addresses.



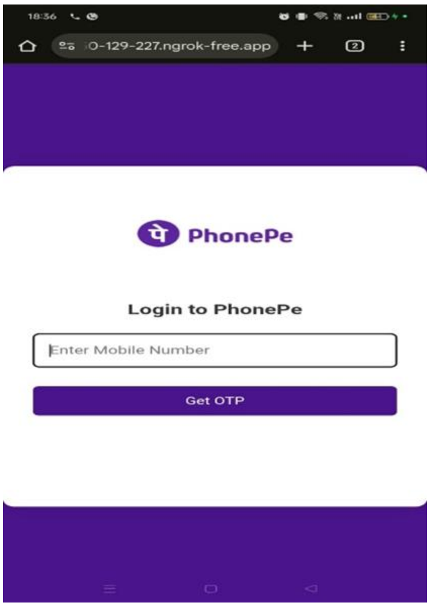
```
ngrok                                                                                   (Ctrl+C to quit)

◆ The Go SDK has reached v2—now simpler, more streamlined, and way more powerful: https://ngrok.com/r/go-sdk-v2

Session Status                online
Account                       nisha (Plan: Free)
Version                       3.23.1
Region                        India (in)
Web Interface                 http://127.0.0.1:4040
Forwarding                    https://06fc-157-50-129-227.ngrok-free.app -> http://localhost:5000

Connections                   ttl     opn     rt1     rt5     p50     p90
                              0       0       0.00    0.00    0.00    0.00
```

Fig 3.8 *— Ngrok Terminal Showing Public HTTPS Tunnel*



Login to PhonePe

Enter Mobile Number

Fig 3.9 *— The Phishing Page Opened in a Mobile Browser*

IV. Result

This project effectively demonstrates how easily users can be tricked into sharing sensitive information such as login credentials, OTPs, and banking details through a fake digital payment interface. A phishing model was carefully designed to replicate the appearance and functionality of the original PhonePe application. Key sections like the login screen, OTP input, and UPI details page were recreated with close attention to detail. By mimicking familiar design elements and leveraging users' trust in the brand, the replica was able to convince participants to unknowingly disclose their private information.

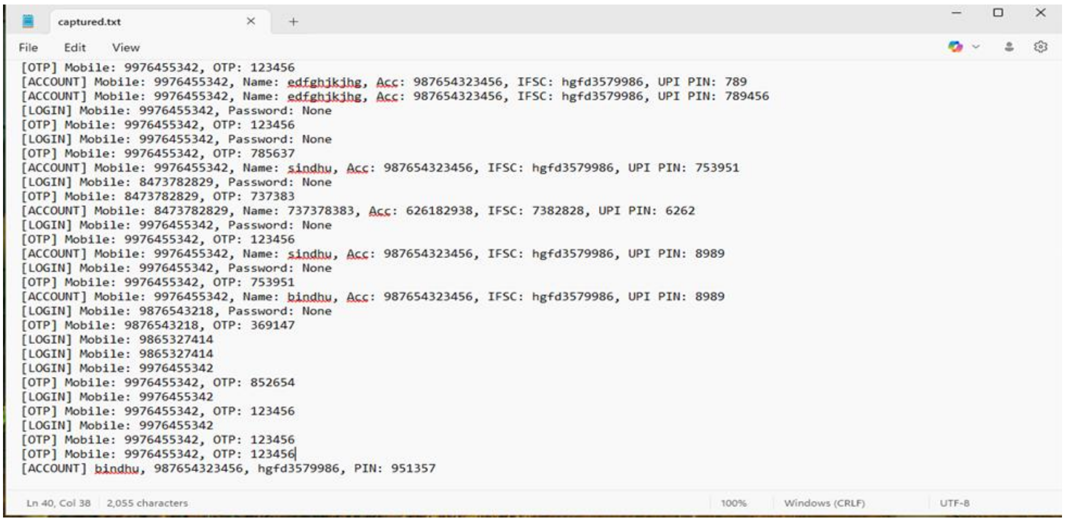
During the testing phase, users interacted with the fake system by entering different types of information, which was safely stored in a backend log file for study. This data collection happened in a secure, controlled setup, following strict ethical rules to make sure no real user data or login details were ever at risk. The demonstration illustrates that phishing does not always require complex malware or skilled hacking. Rather, it can operate simply by deceiving users through clever design and psychological strategies. By mimicking the appearance of genuine websites, fabricating OTP messages with simulated SMS tools, and concealing links via platforms like Cloudflare Tunnel and Bitly, the project effectively replicated typical techniques employed in actual phishing attacks.

The findings of this project reveal critical weaknesses in digital payment systems. Many users were unable to spot small differences in web addresses or layout, particularly when the fake site closely mimicked the design of trusted platforms. The study also points out that single-step security methods, like OTP-based authentication, may not be enough when users can be tricked into sharing their credentials through social engineering. It was also observed that tools intended for legitimate purposes—such as URL shorteners and free web hosting services—can be misused to make phishing attempts appear more credible and far-reaching. To address these challenges, the project suggests several preventive measures:

- Educational programs aimed at increasing awareness of phishing and instructing individuals on identifying suspicious websites.
- Implementing multi-factor authentication (MFA) to reduce reliance on easily phish-able credentials, including biometric data or verification from devices.
- Detection and blocking of phishing attempts in real-time by incorporating AI-driven threat detection technologies into financial applications and web browsers.
- Enhanced cooperation between regulators, technology firms, and cybersecurity organizations to oversee and prevent the misuse of lawful digital instruments.

Alongside the technical findings, this simulation offers a meaningful learning experience for both cybersecurity learners and professionals. It helps deepen the understanding of how attackers think and operate, while also supporting the development of stronger, more practical defense strategies through the safe recreation of real phishing scenarios.

Overall, the project underlines the urgent need for a well-rounded approach to protect digital payment platforms. Raising awareness about user behavior, keeping up with evolving technology, and putting strong policies in place are all key to staying one step ahead of phishing threats.



```
[OTP] Mobile: 9976455342, OTP: 123456
[ACCOUNT] Mobile: 9976455342, Name: edfghjkjhg, Acc: 987654323456, IFSC: hgfd3579986, UPI PIN: 789
[ACCOUNT] Mobile: 9976455342, Name: edfghjkjhg, Acc: 987654323456, IFSC: hgfd3579986, UPI PIN: 789456
[LOGIN] Mobile: 9976455342, Password: None
[OTP] Mobile: 9976455342, OTP: 123456
[LOGIN] Mobile: 9976455342, Password: None
[OTP] Mobile: 9976455342, OTP: 785637
[ACCOUNT] Mobile: 9976455342, Name: sindhu, Acc: 987654323456, IFSC: hgfd3579986, UPI PIN: 753951
[LOGIN] Mobile: 8473782829, Password: None
[OTP] Mobile: 8473782829, OTP: 737383
[ACCOUNT] Mobile: 8473782829, Name: 737378383, Acc: 626182938, IFSC: 7382828, UPI PIN: 6262
[LOGIN] Mobile: 9976455342, Password: None
[OTP] Mobile: 9976455342, OTP: 123456
[ACCOUNT] Mobile: 9976455342, Name: sindhu, Acc: 987654323456, IFSC: hgfd3579986, UPI PIN: 8989
[LOGIN] Mobile: 9976455342, Password: None
[OTP] Mobile: 9976455342, OTP: 753951
[ACCOUNT] Mobile: 9976455342, Name: bindhu, Acc: 987654323456, IFSC: hgfd3579986, UPI PIN: 8989
[LOGIN] Mobile: 9876543218, Password: None
[OTP] Mobile: 9876543218, OTP: 369147
[LOGIN] Mobile: 9865327414
[LOGIN] Mobile: 9865327414
[LOGIN] Mobile: 9976455342
[OTP] Mobile: 9976455342, OTP: 852654
[LOGIN] Mobile: 9976455342
[OTP] Mobile: 9976455342, OTP: 123456
[LOGIN] Mobile: 9976455342
[OTP] Mobile: 9976455342, OTP: 123456
[OTP] Mobile: 9976455342, OTP: 123456
[ACCOUNT] bindhu, 987654323456, hgfd3579986, PIN: 951357
```

Fig 4.1 — Captured credentials of the user**.**

V. Discussion

This research project offers a practical demonstration of a phishing simulation that closely replicates the interface and workflow of a widely used digital payment application, **PhonePe**. The primary aim of this project was to examine the mechanics of phishing attacks from both a technical and psychological viewpoint. It emphasized how cybercriminals exploit user trust by employing visual strategies in the user interface.

The frontend was designed using **HTML and CSS** to enhance the realism of the experience, closely resembling the appearance and feel of the official PhonePe app. This included copying key design elements like fonts, colors, input boxes, and layout. This kind of visual imitation is crucial in making users believe the fake page is genuine, and the project shows how attackers use this to gain trust.

On the backend, the system was created using **Flask**, a lightweight Python framework that handles page routing and form submissions. The fake phishing process followed three main steps that mimic a typical UPI transaction:(1) entering a **mobile number**, (2) **submitting an OTP**, and (3) **entering UPI credentials**. Each step had its own Flask route (such as /login, /otp, and /submit account), which allowed user inputs to be collected in a realistic, step-by-step flow, just like in a real payment session.

User inputs were stored in a local text file named captured.txt, representing the type of data harvesting attackers typically perform in real-world phishing operations. In this simulation, no real data was used only dummy values—for educational and research purposes. However, this data logging mechanism effectively demonstrates how threat actors record and monitor sensitive credentials in real time.

One of the key findings from this simulation is that **visual accuracy and interface similarity alone are often sufficient to deceive users**. This reinforces the idea that phishing attacks do not always depend on complex exploits or malware; rather, **social engineering** and **UI deception** are frequently enough to compromise sensitive information. The project provides a compelling case for how even a basic clone, when convincingly presented, can manipulate users into voluntary data disclosure.

The simulation emphasizes prevalent vulnerabilities on the user side, specifically the tendency of users to overlook essential security indicators such as the **app's source**, the presence of an **SSL certificate**, or the **structure of the website's URL.** Numerous users expose themselves to phishing attempts by failing to verify these details before disclosing sensitive information.

From a technical perspective, the initiative promotes the integration of robust security features directly into essential applications from the outset. This involves incorporating **real-time phishing detection, validating website domains, inspecting credentials on the server side**, and implementing **multi-factor authentication (MFA).** When these measures are consistently and accurately applied, they significantly increase the difficulty for attackers to impersonate or replicate trusted platforms.

In summary, this simulation not only illustrates the execution of a realistic phishing workflow but also provides valuable insights into the **interplay between technology and human psychology** in cybersecurity. The project serves as a **didactic platform** for researchers, educators, and security practitioners, emphasizing the need for **multi-layered security approaches** that combine technical defenses, ethical hacking education, and proactive user awareness.

VI. Conclusion

This project demonstrates that phishing attacks do not necessarily require sophisticated programming techniques or malicious software to succeed. Instead, a well-crafted imitation of a legitimate user interface such as the login and transaction screens of PhonePe can effectively deceive users into disclosing confidential information. By replicating the standard user flow and capturing interactions at each step, the simulation reveals how attackers exploit user trust in familiar visual elements to execute fraudulent activities.

From a technical perspective, the implementation relied on fundamental web technologies and a lightweight backend framework, showcasing how easily phishing kits can be developed and deployed. The integration of a tunnelling service, such as Ngrok, further illustrates the simplicity with which attackers can make deceptive platforms publicly accessible. The project also provided insight into the nature of data users are willing to submit when they perceive the interface to be legitimate.

Importantly, the findings highlight that while security mechanisms such as encryption and multi-factor authentication are essential, they are insufficient if users can be socially engineered into compromising their own data. This reaffirms the notion that the human element often remains the most vulnerable link in cybersecurity.

In an educational context, simulated phishing environments like the one developed in this project serve as effective tools for training and awareness. They enable cybersecurity students, educators, and end-users to explore real-world attack strategies in a safe and controlled setting. Such practical exposure is essential for fostering digital literacy and strengthening defenses against social engineering attacks in today's increasingly digitized financial ecosystem.

VII. Limitations & Future Scope

Limitations: Although the project successfully simulates a phishing attack using a cloned PhonePe interface, it has a few limitations:

- **No Real Backend Verification** The system collects user inputs like mobile numbers and OTPs but does not connect to real backend servers or perform actual authentication, which limits realism.
- **Static Design** The interface is built using basic HTML and CSS without dynamic features like real-time error messages or animations, which are common in real phishing websites.
- **Browser-Based Only** The simulation works only in a web browser and does not cover phishing attacks that happen through mobile apps, such as fake APK files.

Future Scope:

Looking ahead, this project could be expanded in several meaningful directions:

- **Mobile App Simulation** Future versions can include fake mobile apps to study phishing attacks on smartphones more realistically.
- **User Awareness Feedback** The platform can be extended to give users feedback after interaction, helping them learn from their mistakes.
- **Educational Use** The simulation can be used in cybersecurity training programs or workshops to help students and users understand how phishing works in a safe environment.

References

[1] S. Sharma, “A Study On Factors Influencing The User Trust Towards Google Pay,”.

[2] L. Burita, P. Matoulek, K. Halouzka, And P. Kozak, “Analysis Of Phishing Emails,” Aims Electron. Electr. Eng., Vol. 5, No. 1, Pp. 93–116, Mar. 2021, Doi: 10.3934/Electreng.2021006.

[3] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, And K. Kifayat, “A Comprehensive Survey Of Ai-Enabled Phishing Attacks Detection Techniques,” Telecommun. Syst., Vol. 76, No. 1, Pp. 139–154, Jan. 2021, Doi: 10.1007/S11235-020-00733-2.

[4] S. H. Apandi, J. Sallim, And R. M. Sidek, “Types Of Anti-Phishing Solutions For Phishing Attack,” In Iop Conf. Ser.: Mater. Sci. Eng., Vol. 769, Jun. 2020, Doi: 10.1088/1757-899x/769/1/012072.

[5] A. Chaudhuri, “Clone Phishing: Attacks And Defenses,” Int. J. Sci. Res. Publ., Vol. 13, No. 4, Apr. 2023, Doi: 10.29322/Ijsrp.13.04.2023.P13626.

[6] C. S. Eze And L. Shamir, “Analysis And Prevention Of Ai-Based Phishing Email Attacks,” Electronics, Vol. 13, No. 10, P. 1839, May 2024, Doi: 10.3390/Electronics13101839.

[7] “Cybersecurity And Fraud Prevention In India’s Financial Sector: A Comprehensive Review,” Int. J. Creative Res. Thoughts, 2024. [Online]. Available: Www.Ijcrt.Org

[8] Y. S. Enoch, A. K. John, And A. E. Olumuyiwa, “Mitigating Cyber Identity Fraud Using Advanced Multi Anti-Phishing Technique,” Int. J. Adv. Comput. Sci. Appl., 2013. [Online]. Available: Www.Ijacsa.Thesai.Org

[9] S. S. Ravindra, S. J. Sanjay, S. N. A. Gulzar, And K. Pallavi, “Phishing Website Detection Based On Url,” Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., Pp. 589–594, Jun. 2021, Doi: 10.32628/Cseit2173124.

[10] B. Miller, K. Miller, X. Zhang, And M. G. Terwilliger, “Prevention Of Phishing Attacks: A Three-Pillared Approach,” Issues Inf. Syst., Vol. 21, No. 2, Pp. 1–8, 2020, Doi: 10.48009/2_Iis_2020_1-8.

[11] P. Sood And P. Bhushan, “A Structured Review And Theme Analysis Of Financial Frauds In The Banking Industry,” Asian J. Bus. Ethics, Vol. 9, No. 2, Pp. 305–321, Dec. 2020, Doi: 10.1007/S13520-020-00111-W.

[12] J. Milletary, “Technical Trends In Phishing Attacks,”.

[13] B. F. Edburg, K. Umadevi, M. Vidya, P. M. R. Kumar, And B. F. Edburg, “Role Of Upi Application Usage And Mitigation Of Payment Transaction Frauds: An Empirical Study,” Mdim J. Manag. Rev. Pract., Vol. 2, No. 1, Pp. 7–22, 2024, Doi: 10.1177/Mjmrp.231222347.

[14] M. M. Ali And N. F. M. Zaharon, “Phishing—A Cyber Fraud: The Types, Implications And Governance,” Int. J. Educ. Reform, Vol. 33, No. 1, Pp. 101–121, Jan. 2024, Doi: 10.1177/10567879221082966.

[15] K. Beck And J. Zhan, “Phishing In Finance,” In Proc. 5th Int. Conf. Future Inf. Technol. (Futuretech), 2010, Doi: 10.1109/Futuretech.2010.5482704.

[16] W. Yuspin, A. O. Putri, A. Fauzie, And J. Pitaksantayothin, “Digital Banking Security: Internet Phishing Attacks, Analysis And Prevention Of Fraudulent Activities,” Int. J. Saf. Secur. Eng., Vol. 14, No. 6, Pp. 1699–1706, Dec. 2024, Doi: 10.18280/Ijsse.140605.

[17] “Phishing, Pharming And Identity Theft,” Res. Gate, Accessed: Jun. 23, 2025. [Online]. Available: Https://Www.Researchgate.Net/Publication/285678442_Phishing_Pharming_And_Identity_Theft

[18] A. Rao And V. Pillai, “Cybersecurity And Fraud Prevention In India’s Financial Sector: A Comprehensive Review,” J. Indian Financ. Technol., Vol. 6, No. 4, Pp. 70–81, 2022.

[19] M. P. Bach, T. Kamenjarska, And B. Žmuk, “Targets Of Phishing Attacks: The Bigger Fish To Fry,” Procedia Comput. Sci., Vol. 204, Pp. 448–455, Jan. 2022, Doi: 10.1016/J.Procs.2022.08.055.

[20] A. Yadav, “Phishing In India—Analytical Study,” Int. Adv. Res. J. Sci. Eng. Technol., Vol. 8, 2021, Doi: 10.17148/Iarjset.2021.88110.

[21] B. Amro, “Phishing Techniques In Mobile Devices,” J. Comput. Commun., Vol. 6, Pp. 27–35, 2018, Doi: 10.4236/Jcc.2018.62003.

[22] R. Alabdan, “Phishing Attacks Survey: Types, Vectors, And Technical Approaches,” Future Internet, Vol. 12, No. 10, P. 168, Sep. 2020, Doi: 10.3390/Fi12100168.