

## DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (DATA SCIENCE)

**CRYPTOGRAPHY MINI PROJECT REPORT**

Awareness of Phishing Attacks

## SUBMITTED BY

**Palak Rahangdale 4SF21CD019**

## Kavya D Manjrekar 4SF21CD012

**FACULTY IN CHARGE**

## Mrs. SHWETHA SHETTY

**Assistant Professor**

**Department of Information Science (Data Science) SCEM, Mangalore**

# Introduction

Phishing is a social engineering technique where attackers attempt to gain access to sensitive information, such as usernames, passwords, or credit card details, by impersonating a trusted entity. This project has simulated a phishing attack to understand its mechanics and educate users on how to identify and prevent them.

# Phishing Attack Structure

A typical phishing attack follows a well-defined structure:

* + **Reconnaissance:** We have analyzed how attackers gather information about potential targets through social media profiles, data breaches, or malware.
  + **Delivery:** We have examined the methods attackers use to send messages (email, SMS, social media) disguised as a legitimate source (bank, social media platform, etc.).
  + **Phishing Website:** We have designed a mock phishing website to analyze how attackers create fraudulent websites designed to mimic the legitimate website.
  + **Credential Theft:** We have explored how these websites typically prompt the user to enter login credentials or personal information.
  + **Exploitation:** We have discussed how once stolen, the attacker uses the information for unauthorized access to accounts, financial transactions, or identity theft.

# Simulating a Phishing Attack

This section details the creation of a simulated phishing attack, emphasizing ethical considerations:

# Target Selection:

We have avoided targeting specific individuals or organizations. This project focused on understanding the attack mechanics, not exploiting vulnerabilities.

# Message Delivery:

We did not send any phishing messages. Instead, we designed a mock scenario with a sample message.

## Sample Phishing Message (Email):

Subject: Urgent Action Required - Your Account Verification Dear [Username],

This email is to inform you that we have detected suspicious activity on your account. To ensure your account security, please verify your information by clicking the link below and logging in with your username and password.

## Do not ignore this email.

Click here to verify your account: [Phishing Website Link (Placeholder)] Sincerely,

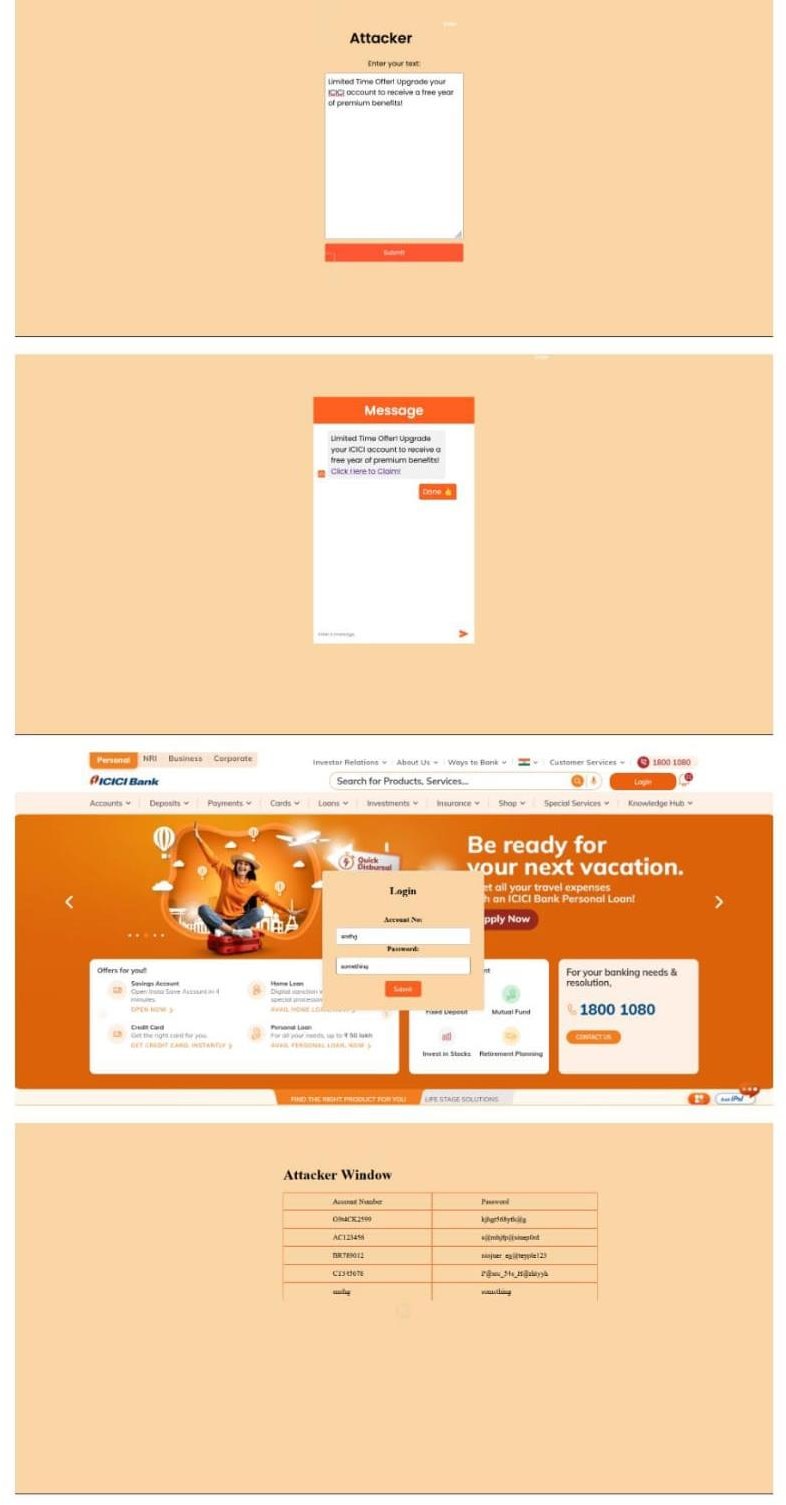
The [ impersonated company name ] Security Team

# Phishing Website Design

We have created a local, non-functional website to simulate the look and feel of the legitimate website. This website has not been hosted online and was only accessible for demonstration purposes.

## Website Design Considerations:

* + - **Visual Similarity:** We mimicked the color scheme, logo, and layout of the legitimate website to understand how attackers create a sense of legitimacy.
    - **Urgency and Scarcity:** We created a sense of urgency by emphasizing the need for immediate action, analyzing how attackers use pressure tactics.
    - **Form Design:** We included login fields for username and password mimicking the legitimate website to understand how attackers capture credentials.
    - **Disclaimers:** We clearly marked the website as a simulation for educational purposes only.



# Identifying Phishing Attacks

## Red Flags:

* + **Sense of Urgency:** Phishing messages often pressure users to act immediately without proper time for verification. We have analyzed how this tactic exploits user emotions.
  + **Generic Greetings:** Legitimate companies usually address users by name. We examined how attackers use generic greetings to cast a wider net.
  + **Suspicious Links:** Hovering over the link before clicking to see the actual URL is crucial. We analyzed how mismatched domains or typos in URLs can be red flags.
  + **Grammatical Errors:** Phishing messages often contain typos or grammatical errors. We identified how such errors can indicate a lack of attention to detail.
  + **Unfamiliar Sender:** Be wary of emails or messages from unknown senders. We emphasized how verifying the sender's identity is essential.

# Preventing Phishing Attacks

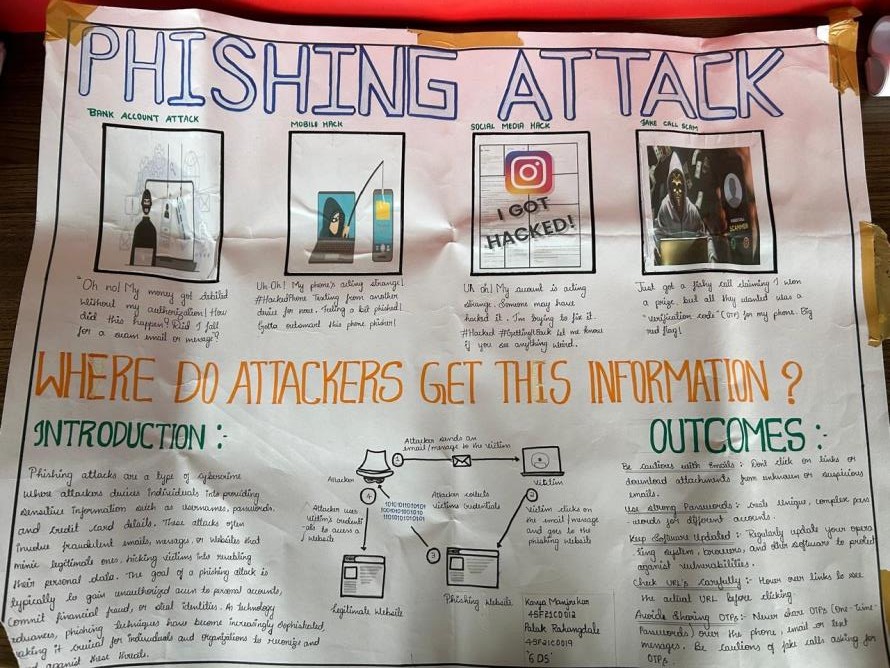
## User Awareness:

* + Educate yourself and others about common phishing tactics.
  + Be skeptical of unsolicited messages, even if they appear legitimate.
  + Verify the sender's identity before clicking on links or opening attachments.
  + Don't enter personal information on suspicious websites.

## Technical Measures:

* + Use strong and unique passwords for all accounts.
  + Enable two-factor authentication (2FA) for added security.
  + Keep your software and operatin
  + g system up to date with security patches.
  + Use anti-phishing and anti-malware software.

## Conclusion:

Phishing attacks remain a significant threat, but this project has empowered us to understand their inner workings. By simulating an attack, we analyzed how attackers target victims, design deceptive websites, and exploit stolen credentials. Recognizing red flags like urgency, generic greetings, and suspicious links is crucial. User education and technical measures like strong passwords and 2FA are vital defenses. This project serves as a valuable tool to raise awareness and empower users to stay safe in the digital landscape.