Experiment–05

5.1 Aim:

Phishing Email Analysis: Develop skills in identifying common indicators of phishing attempts in emails to enhance email security awareness.

5.2 Course Outcome:

Apply email analysis techniques to detect phishing characteristics, understand social engineering tactics, and improve defenses against phishing attacks.

5.3 Lab Objective:

To analyze sample emails for phishing indicators by examining headers, content, URLs, and attachments to differentiate legitimate emails from phishing attempts.

5.4 Requirements:

- Operating System: Windows / Linux / macOS
- Tools:
  - Email client (e.g., Outlook, Thunderbird) or Webmail interface
  - Email header analyzer tools (e.g., MXToolbox, Google's Email Header Analyzer)
  - URL scanner tools (e.g., VirusTotal, URLVoid)
- Sample phishing and legitimate email samples (provided or collected)
- Internet connection for online tools

5.5 Theory:

Phishing is a cyber attack technique where attackers masquerade as trustworthy entities to trick users into revealing sensitive information like passwords, credit card numbers, or installing malware. Phishing emails often contain subtle signs that differentiate them from legitimate communications.

Common Indicators of Phishing Emails:

- Suspicious sender email addresses (misspelled or domain mismatches)
- Generic greetings instead of personalized names
- Urgent or threatening language urging immediate action
- Poor grammar and spelling errors
- Unexpected attachments or links
- URLs with misleading domain names or IP addresses
- Inconsistent email headers or forged SPF/DKIM records

Applications:

- Enhancing user awareness and training
- Email filtering and threat detection

- Incident response and forensics

5.6 Tasks:

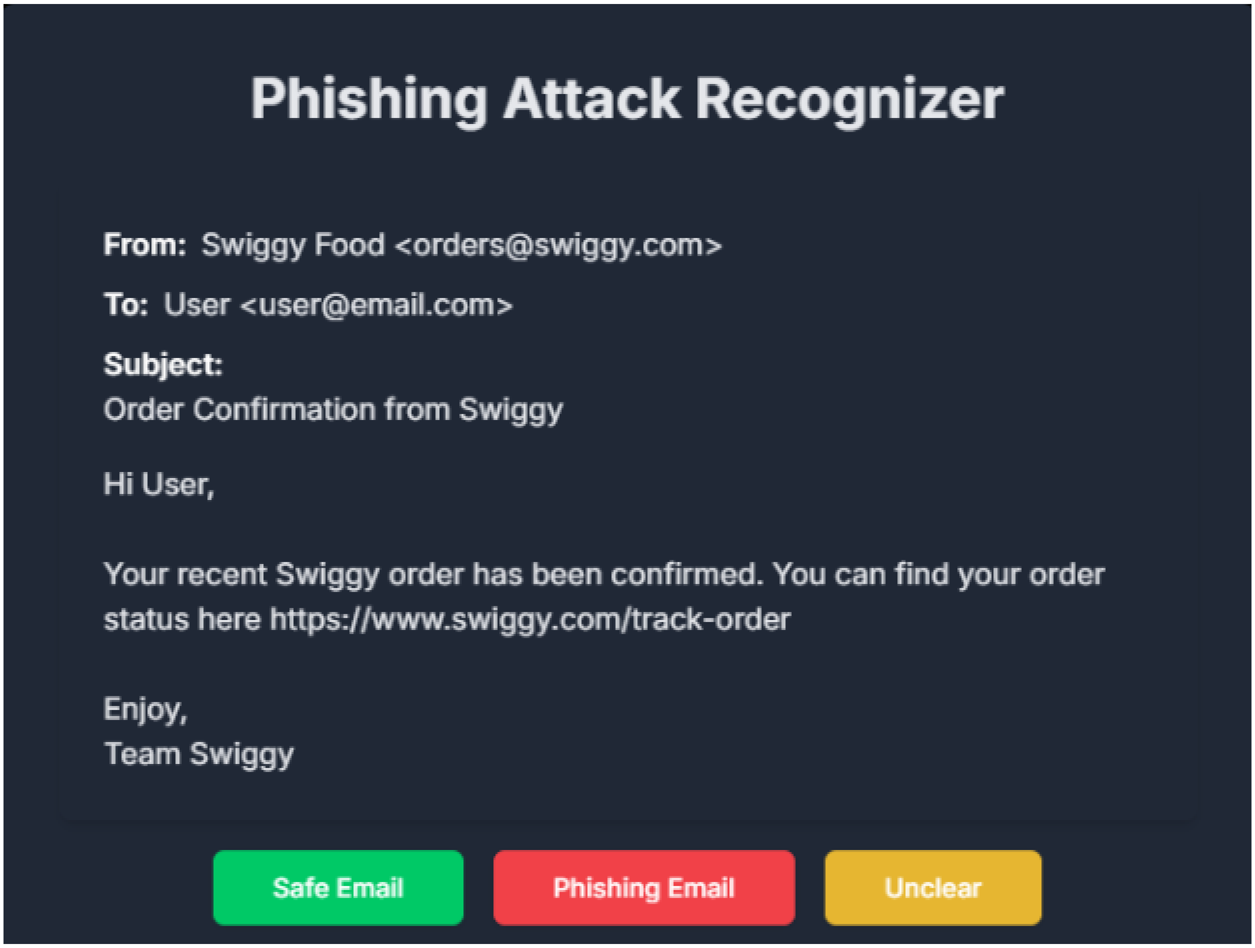
1. Obtain sample phishing and legitimate emails (can be provided or sourced from test datasets).
2. Open an email and examine the sender's email address and display name. Identify any anomalies.
3. View the full email headers and analyze the "Received" path, SPF, DKIM, and DMARC authentication results using header analyzer tools.
4. Analyze the email body for signs such as generic greetings, urgent language, spelling/grammar mistakes, and suspicious formatting.
5. Identify any URLs or hyperlinks in the email, then scan these URLs using online URL scanners for reputation and safety.
6. Inspect attachments for suspicious file types or unexpected content. Do not open attachments on your system if unsure; analyze metadata or use sandbox tools if available.
7. Compare the characteristics of phishing emails with legitimate ones and document key differences.
8. Summarize the phishing indicators found in each analyzed email sample.

5.7 Output Screenshots:

(Add screenshots showing:

- Email header details and analysis results
- Sender email discrepancies
- URL scanning reports
- Phishing email content highlighting suspicious elements
- Comparison with legitimate email content)

Output 1



Phishing Attack Recognizer

From: Swiggy Food <orders@swiggy.com>

To: User <user@email.com>

Subject:
Order Confirmation from Swiggy

Hi User,

Your recent Swiggy order has been confirmed. You can find your order status here https://www.swiggy.com/track-order

Enjoy,
Team Swiggy

Legitimate Email – Swiggy Order Confirmation

Email Header:

- From: orders@swiggy.com — Matches official domain
- To: User's correct email address

Link Check:

- URL: https://www.swiggy.com/track-order — Valid and secure Swiggy link
- No suspicious redirects or typos

Content Check:

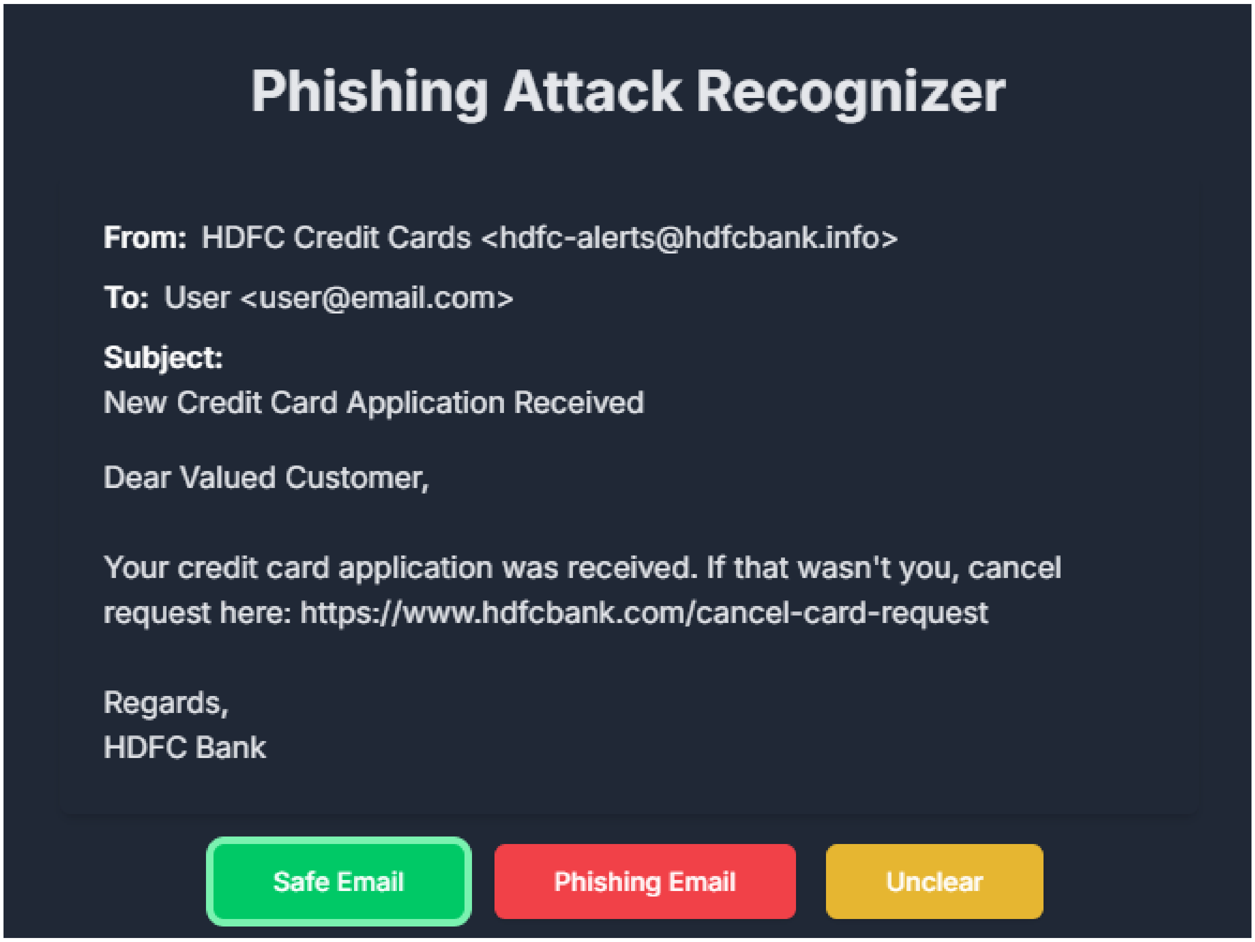
- Subject and body align with typical Swiggy order confirmations
- Language is professional and error-free
- Signed by Team Swiggy

Why It's Safe:

- Verified sender domain
- Secure and correct URL
- No threats, urgency, or misleading claims
- Matches known legitimate format

Verdict: Safe Email

Output 2



Phishing Attack Recognizer

From: HDFC Credit Cards <hdfc-alerts@hdfcbank.info>

To: User <user@email.com>

Subject:
New Credit Card Application Received

Dear Valued Customer,

Your credit card application was received. If that wasn't you, cancel request here: https://www.hdfcbank.com/cancel-card-request

Regards,
HDFC Bank

Phishing Email – Fake HDFC Credit Card Alert

Email Header:

- From: `hdfc-alerts@hdfcbank.info` — **Suspicious domain**
  - **Official HDFC domain is:** `hdfcbank.com`
  - `.info` domain is commonly used in phishing attacks

Link Check:

- Link shown: `https://www.hdfcbank.com/cancel-card-request`
- Actual link (on hover) could lead to a **fake site** despite looking correct
  - Common phishing trick: display a legit URL but hyperlink a fake one

Content Check:

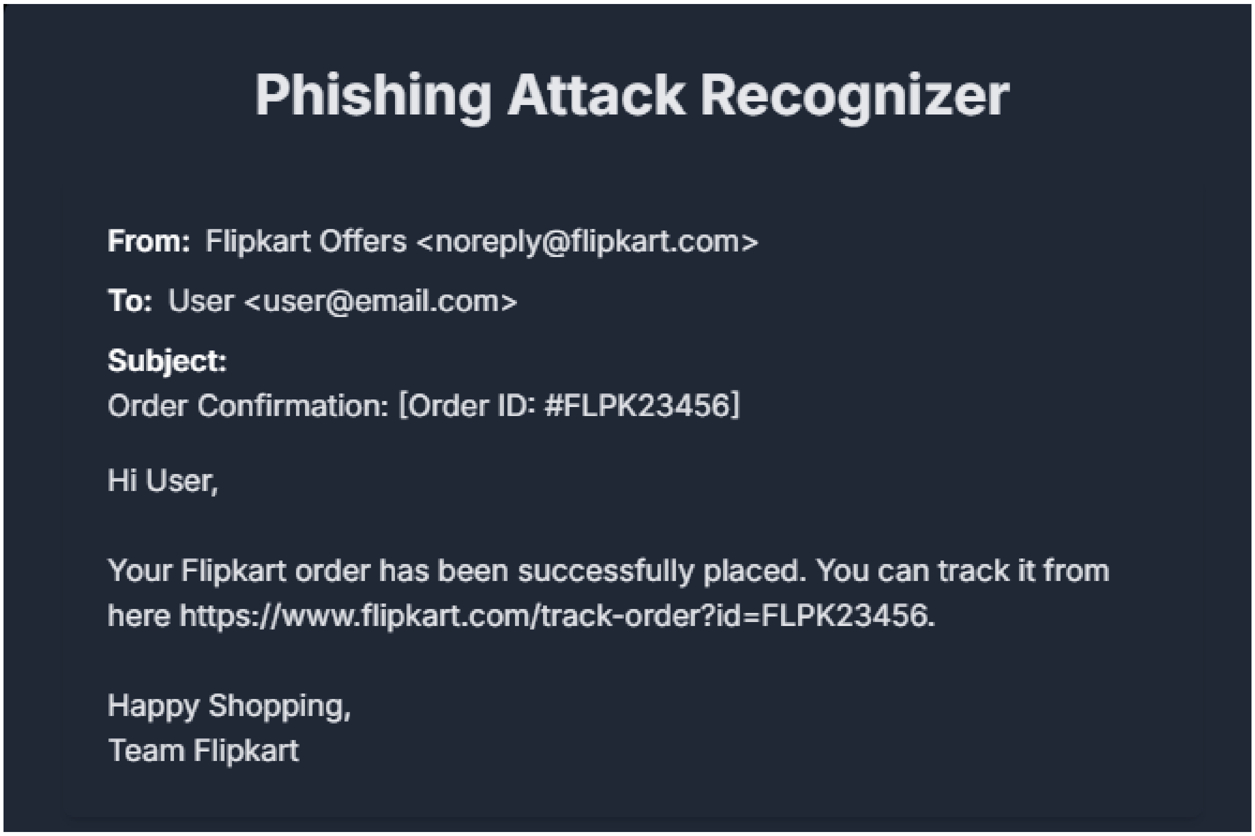
- Generic greeting: “Dear Valued Customer” — real banks usually address by full name
- Creates urgency: “If that wasn’t you, cancel now” — phishing tactic
- No account/application number or personal details

Why It's Phishing:

- Fake domain (`hdfcbank.info`)
- Urgent, fear-based language
- Suspicious link possibly disguised
- Lacks personal/account information

Verdict: Phishing Email

Output 3



Phishing Attack Recognizer

From: Flipkart Offers <noreply@flipkart.com>

To: User <user@email.com>

Subject:
Order Confirmation: [Order ID: #FLPK23456]

Hi User,

Your Flipkart order has been successfully placed. You can track it from here https://www.flipkart.com/track-order?id=FLPK23456.

Happy Shopping,
Team Flipkart

Safe Email – Flipkart Order Confirmation

Email Header:

- From: noreply@flipkart.com — Valid official Flipkart domain
- To: User’s correct email

Link Check:

- URL: https://www.flipkart.com/track-order?id=FLPK23456 — Secure and matches Flipkart domain
- No signs of fake domains or redirects

Content Check:

- Clear subject with order ID
- Language is professional
- Contains expected info: order confirmation, order ID, tracking link
- Signed as Team Flipkart

Why It's Safe:

- Verified sender domain
- HTTPS secure link
- Order-specific information
- Tone and structure match real Flipkart emails

Verdict: Safe Email

5.8 Conclusion:

Through this experiment, we successfully identified and analyzed key indicators of phishing emails by examining sender details, headers, message content, links, and attachments. By comparing phishing samples with legitimate emails, we recognized patterns such as suspicious domains, generic greetings, urgent language, and misleading URLs. This hands-on analysis enhanced our understanding of social engineering tactics and strengthened our ability to detect phishing attempts. As a result, we are now better equipped to assess email authenticity and contribute to stronger email security practices.