Intern

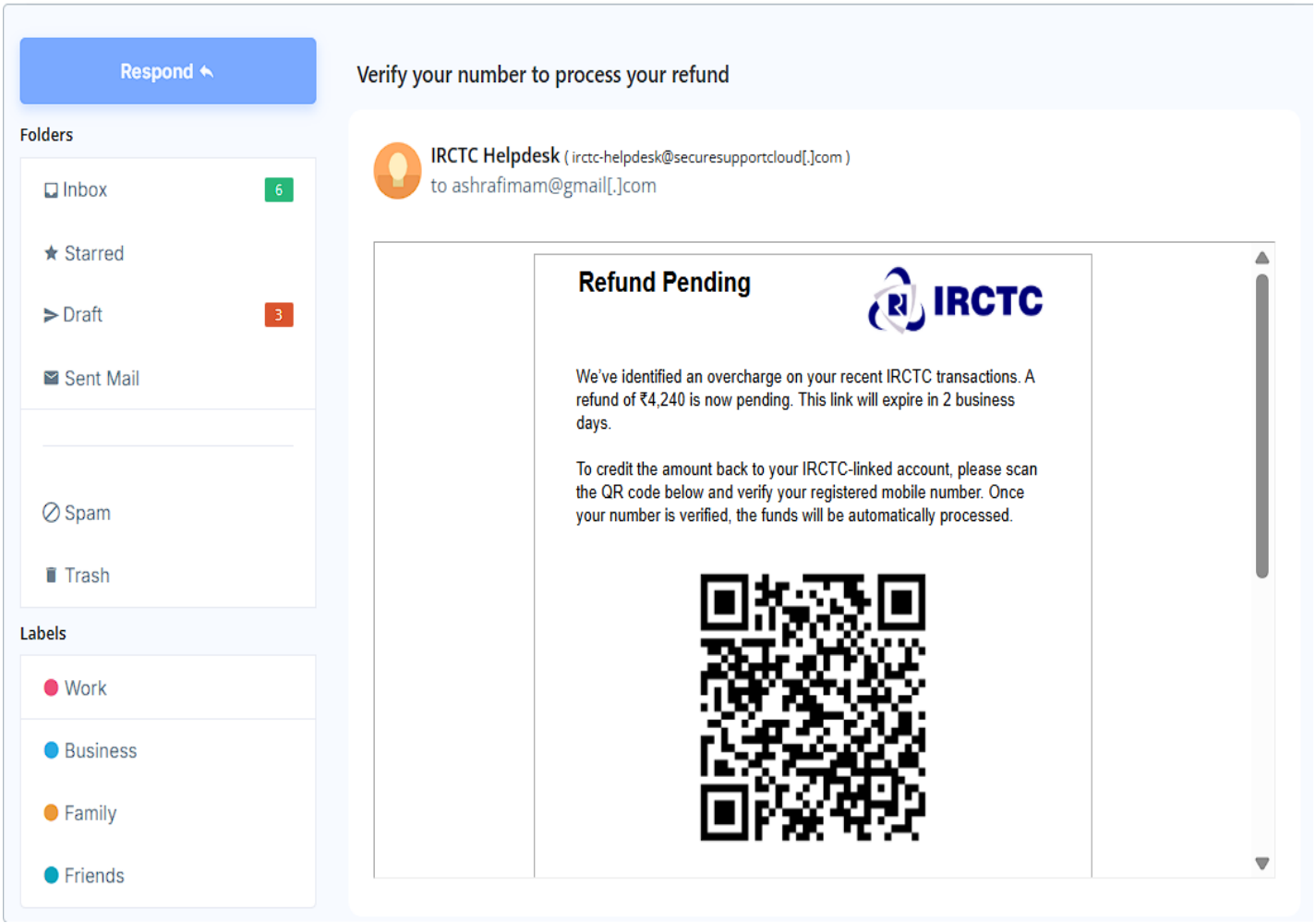
Imam Ashraf
Email: ashrafimam121@gmail.com
Date: 24-06-2025

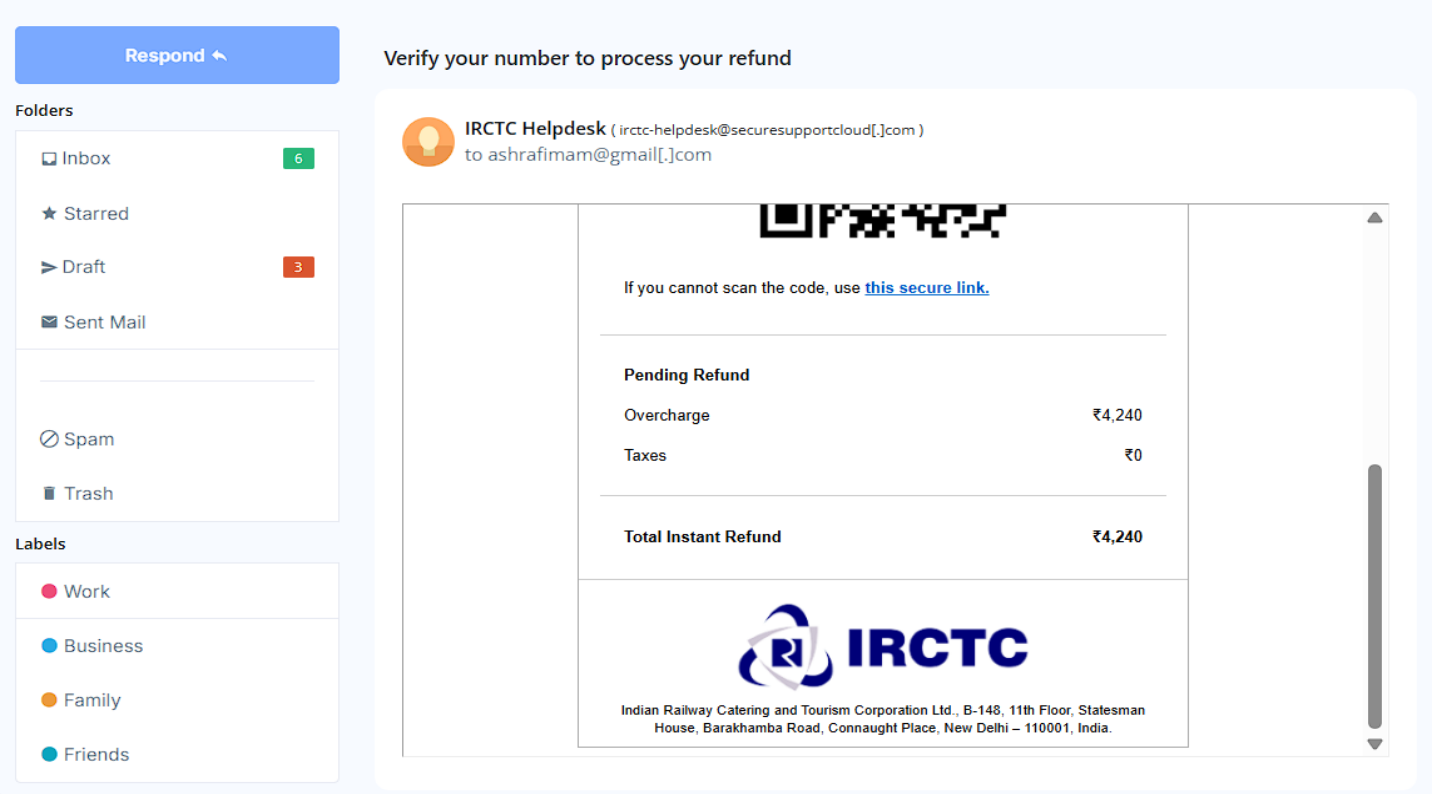
Cyber Security Internship – Task 2

Phishing Email Analysis & Security Awareness Report

Phishing Email Analysis Report – IRCTC Refund Scam

Email Snapshot





Subject: Refund Pending
From: IRCTC Helpdesk <irctc-helpdesk@securesupportcloud.com>
To: ashrafimam@gmail.com
Claim: You're owed a refund of ₹4,240 from IRCTC
Action Required: Scan a QR code or click a secure link to verify mobile number

1. Obtain a Sample Phishing Email

This email mimics a security alert or refund message from IRCTC, a common phishing theme targeting Indian users.

2. Examine Sender's Email Address for Spoofing

Sender: irctc-helpdesk@securesupportcloud.com
Issue: This domain is not affiliated with IRCTC. The official domain is @irctc.co.in.
Phishing Indicator: Spoofed or unrelated domain.

3. Check Email Headers for Discrepancies

SPF and DKIM Information

Headers Found

Header Name	Header Value
Subject	Verify your number to process your refund

Received Header

```
Subject: Verify your number to process your refund


user
IRCTC Helpdesk ( irctc-helpdesk@securesupportcloud[.]com )
to ashrafimam@gmail[.]com.


Refund Pending

We’ve identified an overcharge on your recent IRCTC transactions. A refund of ₹4,240 is now pending. This link will expire in 2 business days.

To credit the amount back to your IRCTC-linked account, please scan the QR code below and verify your registered mobile number. Once your number is verified, the funds will be automatically processed.

If you cannot scan the code, use this secure link.
Pending Refund
Overcharge
₹4,240
Taxes
₹0
Total Instant Refund
₹4,240
```

Likely issues include:
- Failed SPF/DKIM authentication.
- Return-Path shows origin from unknown cloud or foreign server.
- Reply-To might redirect to another malicious address.

Phishing Indicator: Header mismatch and failure of authentication protocols.

4. Identify Suspicious Links or Attachments

Includes a QR code and a “secure” link likely redirecting to a phishing page.
Phishing Indicator: QR code and malicious redirect links.

5. Look for Urgent or Threatening Language

Example: “Refund of ₹4,240 is now pending” and “This link will expire in 2 business days”.
Phishing Indicator: Use of urgency to provoke immediate action.

6. Note Any Mismatched URLs (hover vs real)

Displayed link appears official but redirects to a suspicious domain or IP.
Phishing Indicator: Mismatched or disguised links.

7. Verify Presence of Spelling or Grammar Errors

This phishing email is well-written and free of grammatical errors, which makes it more deceptive.
Phishing Indicator: Polished formatting used to deceive.

8. Summary of Phishing Traits Identified

1. Spoofed Email Address
2. Failed Header Authentication
3. Suspicious QR Code and Links
4. Urgency or Threat
5. Mismatched URLs
6. Polished Language (no grammar mistakes)

Phishing Awareness

1. What is phishing?

Phishing is a type of cyberattack in which attackers trick individuals into revealing sensitive information (like passwords, credit card numbers, or personal data) by posing as a legitimate entity—often through fake emails, websites, or messages. In the IRCTC example, the attacker pretended to offer a refund to trick the user into clicking a malicious link or scanning a QR code.

2. How to identify a phishing email?

You can identify a phishing email by looking for:
- Spoofed sender address (e.g., irctc-helpdesk@securesupportcloud.com is fake)
- Urgent or alarming language (e.g., "Refund will expire in 2 business days")
- Suspicious links or QR codes (hovering reveals mismatched or unknown URLs)
- Spelling/grammar errors (though well-crafted ones may be error-free)
- Unusual requests (asking for personal info or verification through a third-party link)

3. What is email spoofing?

Email spoofing is when attackers forge the "From" address in an email to make it appear as though it came from a trusted source.
In the phishing example, the attacker used the address irctc-helpdesk@securesupportcloud.com, which looks official but is actually unaffiliated with IRCTC.

4. Why are phishing emails dangerous?

Phishing emails are dangerous because they can:
- Steal your sensitive data (login credentials, bank details, etc.)
- Install malware through malicious links or attachments
- Trick you into making payments (like scanning UPI QR codes)
- Bypass security software with clean-looking, well-written content

5. How can you verify the sender's authenticity?

To verify a sender's authenticity:
- Check the domain (e.g., real IRCTC uses @irctc.co.in)
- Hover over links to ensure they point to official websites
- Use a search engine to compare official communication formats
- Look for digital signatures (SPF/DKIM/DMARC checks in headers)
- Contact the organization directly using official contact info

6. What tools can analyze email headers?

Some free tools to analyze and verify email headers:
- MxToolbox Email Header Analyzer (https://mxtoolbox.com/EmailHeaders.aspx)
- Google Admin Toolbox - Message Header (https://toolbox.googleapps.com/apps/messageheader/)
- IPVoid Header Analyzer (https://www.ipvoid.com/email-header-analyzer/)
- Email clients like Gmail and Outlook also allow you to view full headers manually.

7. What actions should be taken on suspected phishing emails?

If you receive a phishing email:
- Do not click any links or download attachments
- Do not scan any QR codes
- Mark it as phishing in your email client (Report → Phishing)
- Forward it to your organization's security team if applicable

- Delete the email after reporting
- Run a virus/malware scan if you interacted with the email

8. How do attackers use social engineering in phishing?

Attackers use social engineering to exploit human behavior—like trust, fear, or urgency—to manipulate victims into taking unsafe actions.
In the IRCTC example:
- They created urgency ("refund expiring in 2 days")
- Faked authority (posing as IRCTC)
- Offered a reward (₹4,240 refund) to tempt the user
- Used a trusted scenario (rail ticket refund) to make the attack believable