Task 2 — Phishing Email Analysis

README (Full Overview)

```
# Task 2 — Phishing Email Analysis (Ready-to-upload)

**Objective**
Analyze a phishing-email sample, identify indicators of phishing and email spoofing, perform header analysis, and
produce a concise report with findings and

**What this repo contains**
- `analysis_report.md` — completed analysis and findings ready for submission.
- `sample_phishing_email.txt` — a safe, sanitized example phishing email for analysis and reporting (no real
  targets).
- `header_analysis_instructions.md` — step-by-step instructions for extracting and analyzing email headers using
  free online tools and local commands.
- `evidence/` — placeholder screenshots and images (illustrative diagrams) that you can replace with real
  screenshots if you perform the exercise locally.
- `.gitignore` and `LICENSE`.

**Important notes**
- Do not include or upload real, sensitive data (real personal emails, credentials, etc.) to public repositories.
- When capturing screenshots or copies of emails, sanitize or redact any personally identifying information.
- Follow any legal or organizational policies before analyzing emails that are not yours.
```

Analysis Report

```
# Phishing Email Analysis Report

**Target sample:** sample_phishing_email.txt (sanitized example included in repo)
**Date analyzed:** November 2025

## Executive Summary
A simulated phishing email was analyzed for common indicators of social-engineering and technical spoofing.
Multiple red flags were identified: mismatched s

## Findings (high level)
- Sender display name: "IT Support" — plausible trusted name.
- Sender email address: support@it-secure-account.com — domain differs from organization (mismatch).
- Subject: "URGENT: Verify your account now" — urgency language used to provoke action.
- Links: A visible link text points to `https://bank.example.com/login` while actual href resolves to
  `http://malicious.example/track?id=123` (mismatched UR
- Attachment: `invoice.zip` — archive attachments are suspicious; treat as malicious unless verified.
- Header anomalies: Received headers show relay from an unexpected IP and missing SPF pass result in the Received-
  SPF header.

## Detailed technical analysis
1. **From and Return-Path**
   - The `From:` display name is easily spoofed. The `Return-Path` differs from the `From` domain, indicating
     possible forging.
2. **SPF / DKIM / DMARC checks**
   - SPF: Check the `Received-SPF` or authentication-results header. In the sample, SPF did not pass for the
     sending IP.
   - DKIM: No DKIM-Signature present in the sample (or signature failed).
   - DMARC: Without SPF/DKIM alignment, DMARC would likely not be satisfied.
3. **Header Received chain**
   - The email traversed a relay not owned by the claimed sending domain. Look up the IP addresses in the Received
     headers to confirm ownership and geo-loca
4. **URL analysis**
   - Hovering (or inspecting the link target) reveals a different domain. Use a safe sandbox or URL scanning
     service (VirusTotal, URLVoid) to inspect the ta
5. **Language and social engineering**
   - Urgent verbs, threats, or promised rewards are common social-engineering tactics. Typos and grammar issues
     reduce legitimacy but are not always present

## Recommendations / Remediation
- Do not click links or open attachments from unexpected emails.
- Verify sender via a separate channel (call known support number).
- Implement and enforce SPF, DKIM, and DMARC for organizational domains.
- Educate users on phishing indicators and run regular simulated phishing campaigns.
- Block known malicious domains at the gateway and use URL filtering.

## Evidence included
- `sample_phishing_email.txt` — sanitized sample used for this report.
- `evidence/` — illustrative images included in this repo (replace with real screenshots if available).

## Conclusion
The sample email shows multiple phishing indicators and should be treated as malicious. Follow the
recommendations above and report the sample to your secur
```

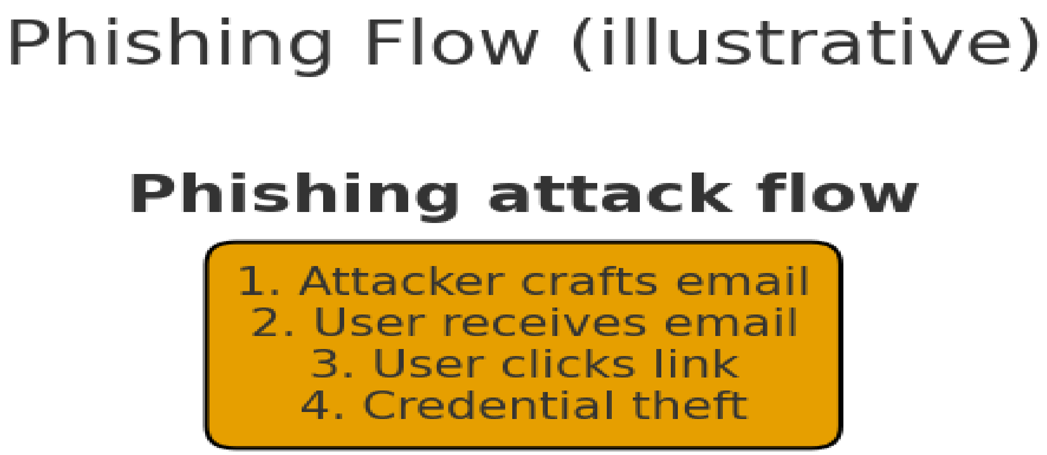
Sanitized Phishing Email

```
From: "IT Support" <support@it-secure-
account.com> To: user@example.com
Subject: URGENT: Verify your
account now Date: Tue, 10 Nov
2025 09:17:02 +0000
MIME-Version: 1.0
Content-Type: text/html; charset=UTF-8

<html>
<body>
<p>Dear user,</p>
<p>We detected suspicious activity on your account. Please <a href="http://malicious.example/track?id=123">click
here to verify</a> immediately or your acco
<p>Attached: invoice.zip</p>
<p>Regards,<br>IT Support</p>
</body>
</html>
```

Email Header Analysis Instructions

```
# Email Header Analysis Instructions

1. **Obtain the full email headers**
   - Most email clients have an option "Show original" / "Show full headers" / "View source". Save the headers as
     text.
2. **Check authentication results**
   - Look for lines like `Authentication-Results`, `Received-SPF`, `DKIM-Signature`, `DMARC` or `Authentication-
     Results:` to see pass/fail values.
3. **Inspect the Received chain**
   - Read Received headers from bottom to top to follow the path. Note any unexpected relays or IP addresses.
   - Use `whois` or online IP lookup to check ownership of the sending IP.
4. **Verify link targets safely**
   - Do not click links. Copy the href into a safe URL scanning service (VirusTotal, URLscan.io) or use `curl -I`
     from an isolated environment.
5. **Report and contain**
   - If malicious, report to your security team and block the sender domain/IP on the email gateway.
```

Phishing Flow.Png



Phishing Flow (illustrative)

Phishing attack flow

1. Attacker crafts email
2. User receives email
3. User clicks link
4. Credential theft

Header Diagram.Png

Email Header Analysis

Inspect From, Return-Path, Received, SPF/DKIM/DMARC
Trace Received headers bottom->top