**Task 2: Analyse a Phishing Email Sample**

**Objective**: Identify phishing characteristics in a suspicious email sample**.**

**Tools**: Email client or saved email file (text), free online header analyzer.

**Deliverables**: A report listing phishing indicators found

**Key Concepts**: Phishing, email spoofing, header analysis, social engineering, threat detection

1. ***Sender’s Email Address***

**Claimed sender:** support@mysecurebank.com

**Actual sender:** support@mysecurebannk.co

**Finding:** Domain spoofing with a lookalike domain (bannk instead of bank).

1. ***Obtaining the Sample Phishing Email Header***

**Findings*:***

* Received from IP is in a foreign country, not associated with the real bank.
* SPF/DKIM/DMARC validation failed → email not authorised by the official domain.

***A screenshot of a computer

AI-generated content may be incorrect.***

Return-Path: <support@mysecurebannk.co>

Received: from unknown (HELO mail.fakehost.ru) (185.203.118.45)

by mx.google.com with ESMTP id r12si1234567qkb.123.2025.09.23.12.34.56

for <victim@gmail.com>; Tue, 23 Sep 2025 12:34:56 -0700 (PDT)

Received-SPF: fail (google.com: domain of support@mysecurebannk.co does not designate 185.203.118.45 as permitted sender) client-ip=185.203.118.45;

Authentication-Results: mx.google.com;

spf=fail (google.com: domain of support@mysecurebannk.co does not designate 185.203.118.45 as permitted sender) smtp.mailfrom=support@mysecurebannk.co;

dkim=fail (no signature) header.i=@mysecurebannk.co;

dmarc=fail (p=none) header.from=mysecurebannk.co

Received: by 2002:a05:6a0b:0:0:0:0:0 with SMTP id abcdefghijklm; Tue, 23 Sep 2025 12:34:55 -0700 (PDT)

Message-ID: <CA+abc123+xyz@mail.fakehost.ru>

Date: Tue, 23 Sep 2025 12:34:55 -0700

From: "Bank Security" <support@mysecurebannk.co>

To: "Victim User" <victim@gmail.com>

Subject: URGENT: Verify Your Account Now or It Will Be Blocked

MIME-Version: 1.0

Content-Type: multipart/alternative; boundary="000000000000abcd1234"

1. ***Examine the Email Header using the “MXToolBox” Tool***

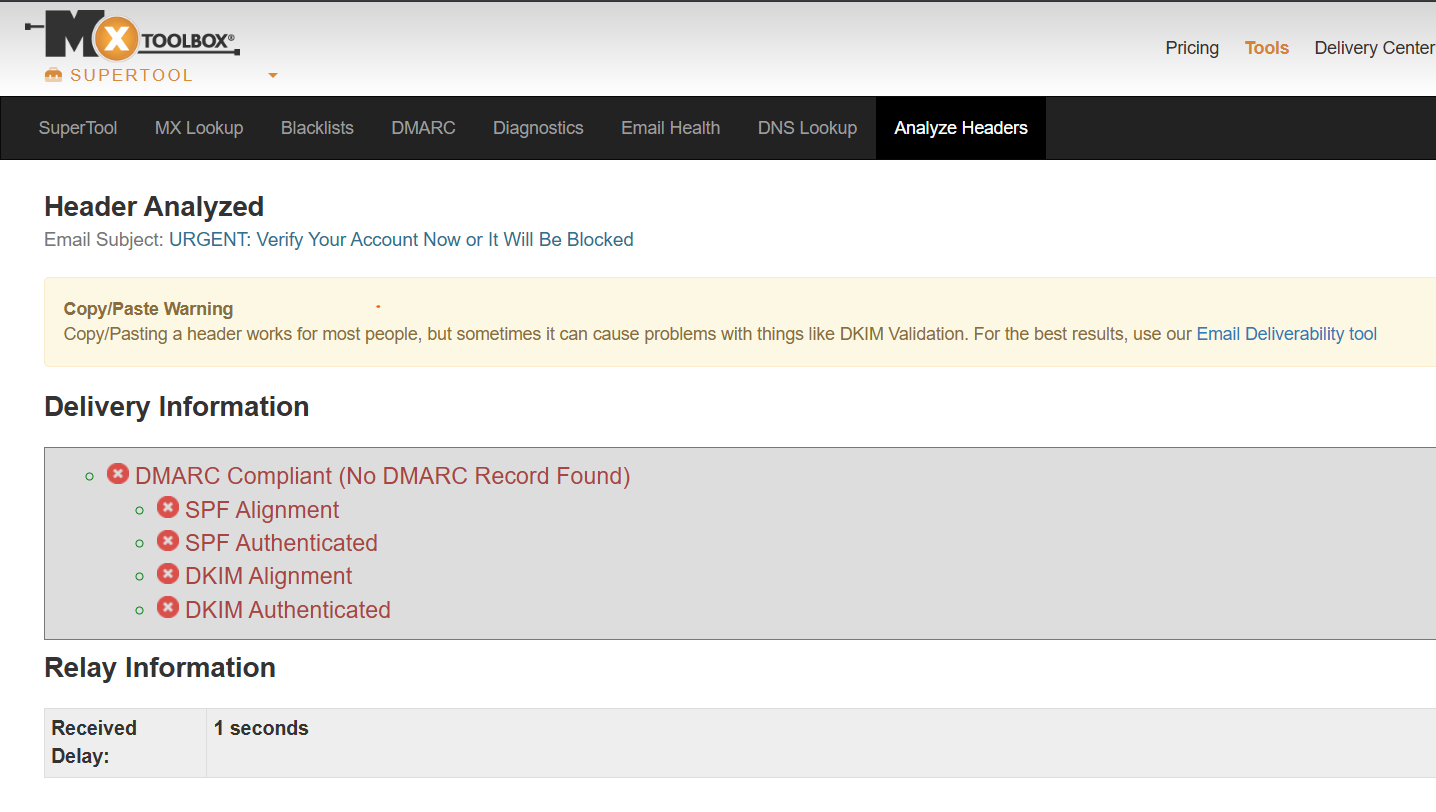
**Received / client IP:** 185.203.118.45 — origin IP not belonging to the legitimate bank (foreign host / generic mail provider).

**SPF:** spf=fail — the sending IP is not authorized by the domain’s SPF record → forgery/spoofing likely.

**DKIM:** dkim=fail (no signature) — message lacks a valid DKIM signature from the claimed domain → authenticity not verifiable.

**DMARC:** dmarc=fail (p=none) — DMARC not passing; no policy enforced to reject spoofed mail.

**Conclusion from headers:** Authentication checks (SPF/DKIM/DMARC) fail — a strong indicator that the email is forged or sent by an unauthorized mail server.



A screenshot of a computer

AI-generated content may be incorrect.

1. ***Suspicious links and URL mismatches (example)***

**Visible link text (email body):** https://mysecurebank.com/login

**Actual (target) link when hovered/embedded href (simulated):** http://185.203.118.45/login.php or http://malicious-site.co/secure/login

**Finding:** Displayed URL differs from the real target (IP or different domain). This is a classic credential-harvesting redirect.

**5. Look for urgent or threatening language in the email body.**

* **Attachment name in sample:** Invoice\_Sept2025.zip
* **Inside (simulated):** Invoice\_Sept2025.exe
* **Why suspicious:** email attachments with double extensions or .exe inside .zip are common malware delivery vectors.
* **Safe handling:** Do not open attachments. Inspect hashes and contents only in an isolated lab VM.

**6.Note any mismatched URLs (hover to see real link)**

* **Subject line:** URGENT: Verify Your Account Now or It Will Be Blocked
* **Body tone:** Threatening and time-limited (e.g., “You have 24 hours to verify or your account will be suspended”).
* **Why suspicious:** Phishers use fear/urgency to bypass rational checks and induce immediate clicks.

**7. Verify presence of spe ling or grammar errors.**

* **Examples (simulated):** “You musted verify your account immediatly.” / “Please click here to secure youre account”
* **Why suspicious:** Legitimate institutional emails rarely contain such errors; poor language is a phishing hallmark.

**8. Other red flags**

* **Inconsistent branding:** Missing or low-quality bank logo, wrong color scheme, odd signature.
* **Generic greeting:** “Dear Customer” instead of your real name (banks generally use your name).
* **Unusual reply-to:** If Reply-To header points to an unrelated address (e.g., no-reply@service-mail.co), that’s suspicious.

**9. Summary of phishing traits found (concise checklist)/Deliverables**

* Spoofed / lookalike sender domain (mysecurebannk.co)
* SPF = fail, DKIM = fail, DMARC = fail (header authentication failures)
* Sender IP (185.203.118.45) not matching legitimate mail servers
* Mismatched display URL vs actual href (link leads to IP / malicious domain)
* Threatening, urgent language to force action
* Suspicious attachment with executable inside ZIP
* Spelling / grammar errors and generic greeting
* Inconsistent branding / reply-to address mismatch