**Phishing Email Analysis Report**

**1. Objective**

The purpose of this task is to analyze a sample phishing email and identify common phishing indicators. This helps build awareness of email-based threats and develops basic threat analysis skills.

### ****2. Tools Used****

* Sample phishing email (text format)
* MXToolbox Email Header Analyzer (https://mxtoolbox.com/EmailHeaders.aspx)
* Manual inspection (hovering over links, reading content)

**3. Sample Phishing Email**

Subject: Urgent: Verify Your Account Now

From: Support@SBIbank-alerts.com

Dear Customer,

Your account has been flagged for suspicious activity.

Please verify your identity immediately by clicking the link below:

https://SBIbank-alerts.com.verify-user.info

Failure to act will result in account suspension.

Thank you,

Your Bank Security Team

**4. Phishing Indicators Found**

| **No.** | **Indicator** | **Description** |
| --- | --- | --- |
| **1** | **Spoofed Email Address** | **The sender uses Support@SBIbank-alerts.com, which is not a verified domain. Legitimate emails from the bank would come from something like @SBIbank.com.** |
| **2** | **Suspicious Link** | **The hyperlink shown is https://SBIbank.com.verify-user.info. It appears to be legitimate but actually redirects to a phishing site.** |
| **3** | **Urgent/Threatening Language** | **The message includes scare tactics such as “account has been flagged” and “failure to act will result in suspension.”** |
| **4** | **Generic Greeting** | **The email uses “Dear Customer” instead of the recipient’s real name. Legitimate services usually personalize emails.** |
| **5** | **Grammar/Style Issues** | **While not full of errors, the tone and structure of the message are slightly unnatural and generic.** |
| **6** | **Mismatched URL** | **The link text may look like it goes to https://SBIbank.com, but when you hover over it, the real destination is https://SBIbank.com.verify-user.info, which is a completely different and suspicious domain.** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |

**Testing a fake email header :**

**Fake Email Header :**

Return-Path: <support@SBIbank-alerts.com>

Received: from unknown (HELO user-pc) (203.0.113.45)

by mail.example.com with SMTP; Mon, 27 May 2025 09:21:53 +0000

Received-SPF: softfail (example.com: domain of transitioning support@SBIbank-alerts.com does not designate 203.0.113.45 as permitted sender)

From: "SBI Support" <Support@SBIbank-alerts.com>

Reply-To: verify@secure-sbiclients.info

To: victim@example.com

Subject: Urgent: Verify Your Account Now

Date: Mon, 27 May 2025 09:21:50 +0000

Message-ID: <87435dfg6sdfg@example.com>

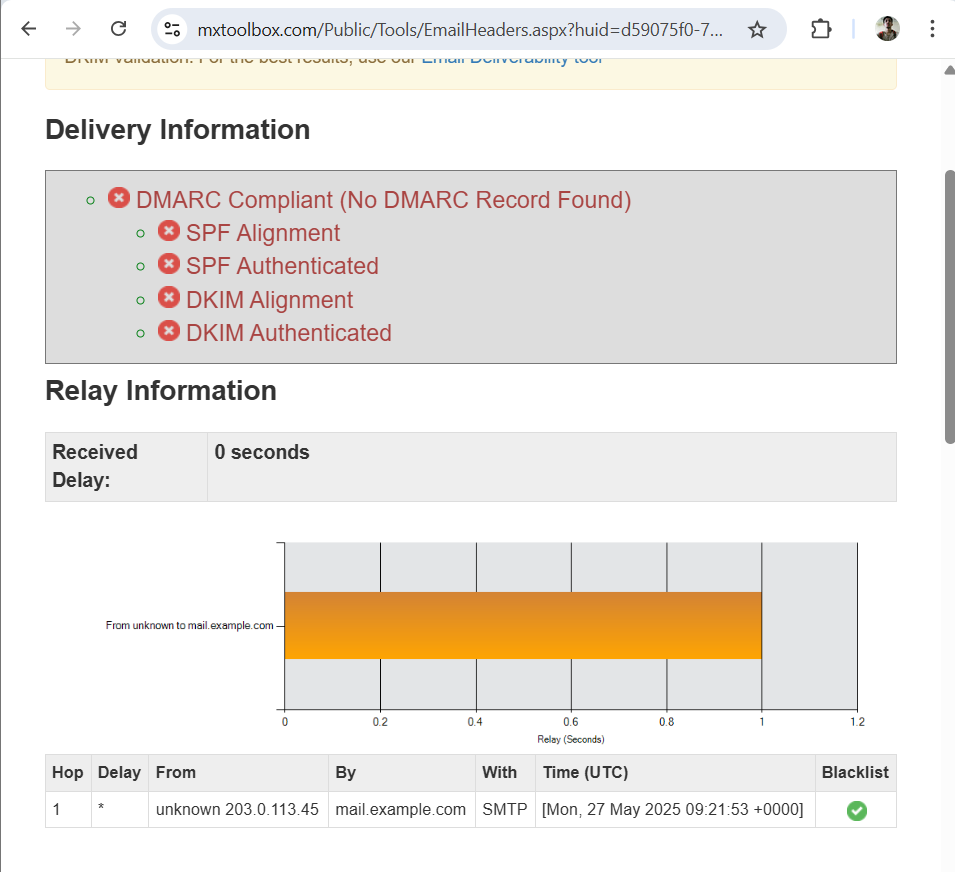
MIME-Version: 1.0

Content-Type: text/html; charset=UTF-8

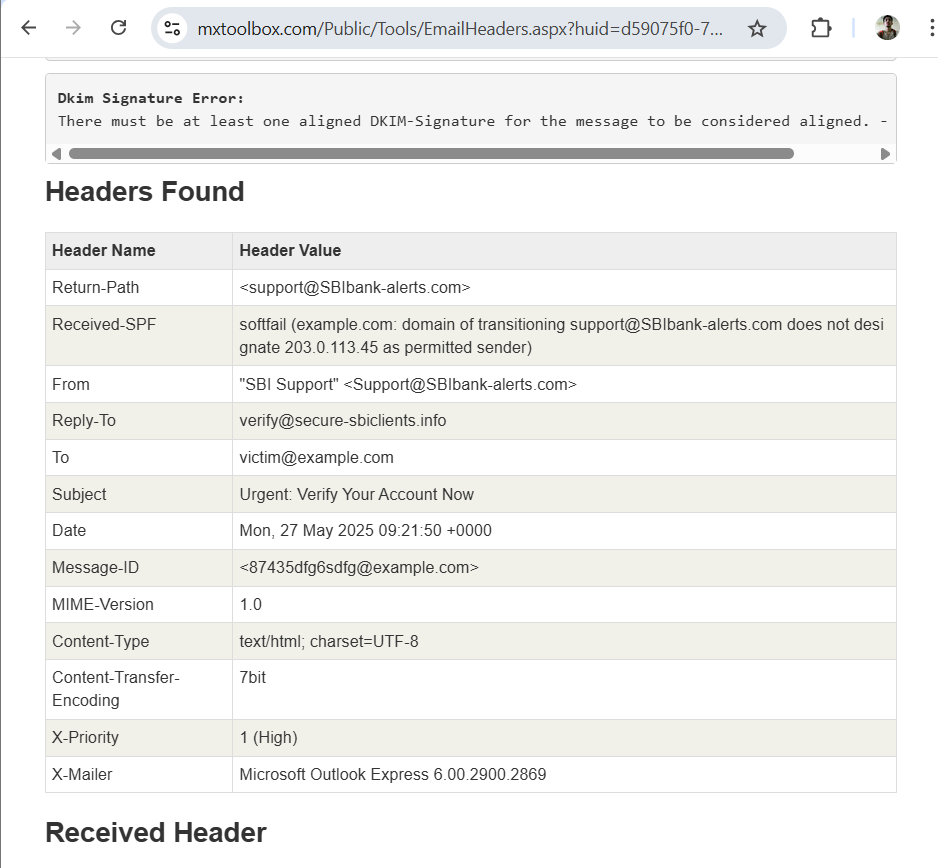
Content-Transfer-Encoding: 7bit

X-Priority: 1 (High)

X-Mailer: Microsoft Outlook Express 6.00.2900.2869



**Analyzing Email Header for discrepancies using mxtoolbox.com free header analyzer**



**Screenshot of header analysis from mxtoolbox.com**

### ****Red Flags in the Email Header:****

1. **Spoofed Sender Domain**  
   From: Support@SBIbank-alerts.com – Looks like a real bank but uses a fake domain.
2. **Reply-To Mismatch**  
   Reply-To: verify@secure-sbiclients.info – Different from sender domain, often used to collect replies.
3. **Suspicious Sending Host**  
   Received: from user-pc (203.0.113.45) – Sent from a non-corporate, likely compromised device.
4. **Urgent Subject Line**  
   Subject: Urgent: Verify Your Account Now – Creates panic to trick the user into acting quickly.
5. **Unusual Mail Client**  
   X-Mailer: Microsoft Outlook Express 6.00.2900.2869 – Outdated client often used in phishing.

### ****Conclusion****

This phishing email demonstrates multiple red flags including a spoofed sender address, mismatched URLs, urgent language, and a suspicious email header. Through this analysis, I have gained practical awareness of phishing tactics and the techniques used to identify and report them.