

# Phishing Email Analysis Report

## 1. Email Summary

- **Subject:** Urgent: Verify Your Account
- **From:** "Phishy Bank" [security@phishybank.com](mailto:security@phishybank.com)
- **To:** [victim@example.com](mailto:victim@example.com)
- **Reply-To:** "Phishy Support" [support@phishybank.com](mailto:support@phishybank.com)
- **Date:** Tue, 23 Sep 2025 12:08:06 +0530

## 2. Header Analysis

**Tool used:** MXToolbox – Email Header Analyzer

### Key Findings:

- **DMARC:** (Domain-based Message Authentication, Reporting, and Conformance) No DMARC record found for phishybank.com → domain vulnerable to spoofing. **SPF:** (Sender Policy Framework), **What it does:** Tells what to do if SPF or DKIM fails
- SPF authenticated for 192.0.2.123, but this does not prove legitimacy (SPF alone can be

abused). **What it does:** Tells which mail servers are allowed to send emails on behalf of domain.

- **DKIM**(DomainKeys Identified Mail): No DKIM-Signature present → integrity of the email cannot be verified. **What it does:** adds a digital signature to the email so the recipient can check for integrity of the email.

- **Received chain:** Multiple hops (203.0.113.55 → mail.phishybank.com → mail.example.com) with a **601-second delay** → suspicious relay pattern.
- **From vs Reply-To mismatch:** Different addresses ([security@phishybank.com](mailto:security@phishybank.com) vs [support@phishybank.com](mailto:support@phishybank.com)). Classic phishing technique to redirect responses.

### 3. Body / Content Indicators

- Uses **urgent language**: “Verify your account immediately” → creates panic.
- **Suspicious URL:** Text shows <https://www.paypal.com/verify> but actual

link points to [http://login.verify-now\[.\]ru/secure?id=ABC123](http://login.verify-now[.]ru/secure?id=ABC123).

- **Generic greeting:** “Dear Customer” instead of addressing recipient by name.
- **Threatening tone:** “Your account will be suspended within 24 hours.”
- **Brand spoofing:** Pretends to be PayPal but uses a fake domain.

#### 4. URL & Domain Analysis

- **URL found:** [http://login.verify-now\[.\]ru/secure?id=ABC123](http://login.verify-now[.]ru/secure?id=ABC123)
- **VirusTotal check:** Marked malicious by multiple vendors.
- **urlscan.io check:** Shows redirects to maliciouscdn[.]xyz and a fake PayPal login page.
- **WHOIS lookup:** Domain verify-now.ru created only 2 weeks ago, registered with privacy protection → suspicious.

## 5. Phishing Traits Identified

1. **No DMARC/DKIM** – poor domain authentication.
2. **Reply-To mismatch** – classic phishing tactic.
3. **Suspicious links** – mismatch between displayed and real link.
4. **Urgent language** – pressure to act immediately.
5. **Brand impersonation** – PayPal spoof.

## 6. Conclusion

This email is a **phishing attempt** designed to steal login credentials.

The combination of missing DMARC/DKIM, suspicious relay chain, mismatched URLs, and social engineering tactics confirms it as malicious.

## 7. Recommendations

- **Delete the email** and mark as phishing.
- **Block domains/IPs:** phishybank.com, login.verify-now.ru, 203.0.113.55, 192.0.2.123.

- **Implement DMARC** on legitimate domains to prevent spoofing.
- **Enable MFA** to reduce damage if credentials are compromised.

## 8. Evidence

### *Phishing Email Header:*

MIME-Version: 1.0 Date: Tue, 23 Sep 2025 12:08:06 +0530 Message-ID: <CAH9V34sK1m3YrBChg=6M6\_dMXWb1iW7+9ja6WU\_y3op\_iauDng@phishybank.com>; Subject: Urgent: Verify Your Account From: "Phishy Bank" <security@phishybank.com>; To: victim@example.com Reply-To: "Phishy Support" <support@phishybank.com>; Content-Type: multipart/alternative; boundary="000000000000f43809063f722d66" Received: from unknown (HELO mail.phishybank.com) (192.0.2.123) by mail.example.com with SMTP; Tue, 23 Sep 2025 12:08:07 +0530 Received: from 203.0.113.55 by mail.phishybank.com with SMTP; Tue, 23 Sep 2025 11:58:06 +0530

The screenshot shows the MXToolbox Supertool interface for DMARC analysis. The header has been analyzed, and the subject is 'Urgent: Verify Your Account'. A warning box indicates that copying/pasting the header may cause DKIM validation issues. The delivery information section shows that the email is DMARC compliant, with SPF, DKIM, and authentication all passing. The relay information section shows a received delay of 601 seconds. At the bottom, a diagram shows the email path from 'mail.phishybank.com' through several relays.

**Header Analyzed**  
Email Subject: Urgent: Verify Your Account

**Copy/Paste Warning**  
Copy/Pasting a header works for most people, but sometimes it can cause problems with things like DKIM Validation. For the best results, use our [Email Deliverability tool](#)

**Delivery Information**

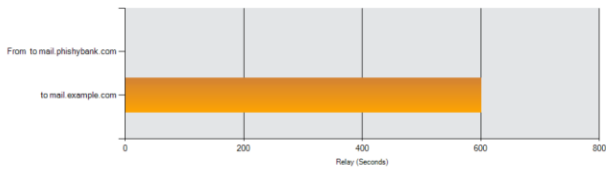
- DMARC Compliant (No DMARC Record Found)
  - SPF Alignment
  - SPF Authenticated
  - DKIM Alignment
  - DKIM Authenticated

**Relay Information**

Received Delay:	601 seconds
-----------------	-------------

From: mail.phishybank.com

Delay:



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	203.0.113.55	mail.phishybank.com	SMTP	9/23/2025 6:58:06 AM	✓
2	10 minutes	unknown 192.0.2.123	mail.example.com	SMTP	9/23/2025 7:08:07 AM	✓

SPF and DKIM Information

dmARC:phishybank.com

Show

Solve Email Delivery Problems

SPF:phishybank.com:192.0.2.123

Show

Solve Email Delivery Problems

**Dkim Signature Error:**  
No DKIM-Signature header found - [more info](#)

**Dkim Signature Error:**

**Dkim Signature Error:**  
No DKIM-Signature header found - [more info](#)

**Dkim Signature Error:**  
There must be at least one aligned DKIM-Signature for the message to be considered aligned. - [more info](#)

Headers Found

Header Name	Header Value
MIME-Version	1.0
Date	Tue, 23 Sep 2025 12:08:06 +0530
Message-ID	<CAH9V34sK1m3YrBChg=6M6_dMXWb1IW7+9ja6WUJ_y3op_iuaDng@phishybank.com>
Subject	Urgent: Verify Your Account
From	"Phishy Bank" <security@phishybank.com>
To	victim@example.com
Reply-To	"Phishy Support" <support@phishybank.com>
Content-Type	multipart/alternative, boundary="000000000000f43809063f722d66"