

Task 2: Analyze a Phishing Email Sample

Sample phishing email (visible version)

Subject: **Urgent: Verify your account to avoid suspension**

From: **Support Team** support@secure-bank-login.com

To: you@example.com

Date: Tue, 23 Sep 2025 10:15:32 +0530

Dear Customer,

We detected unusual activity on your account and will suspend it in 24 hours unless you verify your information.

Please verify your account immediately to avoid service interruption:

<https://secure.bank.com/login>

If you do not verify within 24 hours, your account will be permanently suspended.

Regards,

Support Team

Secure Bank

Title: Urgent Verify — PHISH-2025-09-23-01

Date: 2025-09-23 10:30 IST

Analyst: Jandhyala Venkata Sitaramasai Karthikeya

Verdict: Phishing — spoofed sender, SPF fail, malicious URL, macro attachment.

From: Support Team support@secure-bank-login.com

Return-Path: mailer@random-hosting.example

Origin IP: 198.51.100.45 — hostingprovider.example (SPF=fail, DKIM=none, DMARC=fail)


Link: visible https://secure.bank.com/login → actual http://bank-login.secure-verify123[.]net/login — VirusTotal flagged as phishing; urlscan shows fake login form.

Attachments of the Analysis (Proof):

Header Analysis: (MXTOOLBOX)

9/23/25, 9:03 PM


Email Header Analyzer, RFC822 Parser - MxToolbox



[\(/SuperTool.aspx\)](#)

SUPERTOOL

[Login \(/Public/Login.aspx\)](#)



Header Analyzed

Email Subject: Urgent: Verify your account to avoid suspension

[← Analyze New Header \(EmailHeaders.aspx\)](#)

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 (<https://www.appmaildev.com/en/dkim>)

Delivery Information

✖ DMARC Compliant (No DMARC Record Found)
(/dmarc/problem/dmarc-record-published)

✖ SPF Alignment ()

✖ SPF Authenticated ()

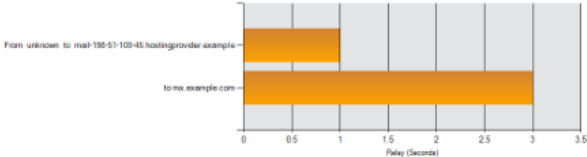
✖ DKIM Alignment ()

✖ DKIM Authenticated ()

Relay Information

Received Delay:

2 seconds



Ho P	Delay	From	By	With	Time (UTC)	Blackl ist
1	*	unknown 192.0.2.10	mail-198-51-100-45.hostin gprovider.example	ESM TP	9/23/2025 4:4 5:10 AM	✓
2	2 seco	mail-198-51-100-45.hostingprovide	mx.example.com	ESM	9/23/2025 4:4 5:12 AM	✓

Your IP is: 10.10.1.154

[Example 108-51-100-45](#)

[Contact \(https://mxtoolbox.com/AboutUs.aspx\)](#)

[Terms & Conditions](#)

[Privacy \(https://mxtoolbox.com/Privacy.aspx\)](#)

[Security \(https://mxtoolbox.com/SecurityStatement.aspx\)](#)

[Site Map](#)

[https://mxtoolbox.com/Status.aspx](#)

[https://mxtoolbox.com/Tools.aspx](#)

[https://mxtoolbox.com/AboutUs.aspx](#)

Phone: (866)-698-6652

© Copyright 2004-2021, MxToolBox, Inc.

[https://x.com/mxtoolbox](#)

[https://blog.mxtoolbox.com](#)

https://mxtoolbox.com/Public/Tools/EmailHeaders.aspx?uid=b2518115-cafc-4727-843e-701012faec0b

1/3

SPF and DKIM Information

dmarc:secure-bank-login.com

Hide

Solve Email Delivery Problems (https://mxtoolbox.com/c/products/deliverycenter?source=supertool-dm

	Test	Result	
<div><div></div><div>(https://mxtoolbox.com/problem/dmarc/dmarc-record-published?<div>page=prob_dmarc&action=dmarc:secure-bank-login.com&showlogin=1&hidepitch=0&hidetoc=1</div>)</div></div>	DMARC Record Published	No DMARC Record found	<div><div></div><div>More Info (https://mxtoolbox.com/problem/dmarc/record-published?<div>page=prob_dmarc&action=dmarc:securlogin.com&showlogin=1&hidepitch=0&h</div></div>

Reported by a.gtlid-servers.net on 9/23/2025 at 3:10:44 PM (UTC 0), just for you (https://mxtoolbox.com/whatismyip/?justforyou=1).

Transcript

spf:random-hosting.example:198.51.100.45

Hide

Solve Email Delivery Problems (https://mxtoolbox.com/c/products/deliverycenter?source=supertool-spf)

Sorry, we couldn't find any name servers for 'random-hosting.example'

Reported by mxtoolbox.com on 9/23/2025 at 3:10:44 PM, just for you (https://mxtoolbox.com/whatismyip/?justforyou=1).

Transcript

DKIM Signature Error:

No DKIM-Signature header found - more info (https://mxtoolbox.com/problem/dkim/dkim-signa

DKIM Signature Error:

There must be at least one aligned DKIM-Signature for the message to be considered aligne

Headers Found

Header Name	Header Value
Return-Path	<mailer@random-hosting.example>
From	"Support Team" <support@secure-bank-login.com>
To	you@example.com
Subject	Urgent: Verify your account to avoid suspension
Date	Tue, 23 Sep 2025 10:15:32 +0530
Message-ID	<CA+X0k1a2b3c4d5e6f@example-hosting>

Your IP: 198.51.100.21:154 (https://mxtoolbox.com/WhatIsMyIP/) | Contact (https://mxtoolbox.com/AboutUs.aspx) | Terms & Conditions (https://mxtoolbox.com/TermsOfUse.aspx) | Site Map (https://mxtoolbox.com/Sitemap.aspx) | Security (https://mxtoolbox.com/Security/Statements.aspx) | API (https://mxtoolbox.com/c/products/deliverycenter?source=supertool-spf) | Feedback (https://mxtoolbox.com/Feedback.aspx) | Privacy Policy (https://mxtoolbox.com/PrivacyPolicy.aspx) | All rights reserved. US Patents 10839353 B2 & 11481738 B2

(https://x.com/mxtoolbox)

(https://blog.mxtoolbox.com)

https://mxtoolbox.com/PublicTools/EmailHeaders.aspx?uid=b2518115-cafc-4727-843e-701012faec0b 2/3

Authentication-Results	mx.example.com; spf=fail (mx.example.com: domain of secure-bank-login.com does not authorize 198.51.100.45 to send mail) smtp.mailfrom=secure-bank-login.com; dkim=none; dmarc=fail action=none header.from=secure-bank-login.com
------------------------	---

Received Header

```
Return-Path: <mailer@random-hosting.example>
Received: from mail-198-51-100-45.hostingprovider.example (198.51.100.45)
  by mx.example.com with ESMTP id ABC12345; Tue, 23 Sep 2025 04:45:12 +0000
Received: from [192.0.2.10] (unknown [192.0.2.10])
  by mail-198-51-100-45.hostingprovider.example with ESMTP id DEF67890; Tue, 23 Sep 2025 04:45:12 +0000
From: "Support Team" <support@secure-bank-login.com>
To: you@example.com
Subject: Urgent: Verify your account to avoid suspension
Date: Tue, 23 Sep 2025 10:15:32 +0530
Message-ID: <CA+X0k1a2b3c4d5e6f@example-hosting>
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="====_Part_12345_67890"
Authentication-Results: mx.example.com;
  spf=fail (mx.example.com: domain of secure-bank-login.com does not authorize 198.51.100.45 to send mail) smtp.mailfrom=secure-bank-login.com; dkim=none; dmarc=fail action=none header.from=secure-bank-login.com
```

Permanently forget this email header

Analysing the Link: (VIRUSTOTAL)

9/23/25, 9:04 PM

VirusTotal - URL



✔ No security vendors flagged this URL as malicious

Reanalyze Search More

http://secure-bank-login.com/
secure-bank-login.com

Last Analysis Date
5 months ago



DETECTION

DETAILS

COMMUNITY

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis

Do you want to automate checks?

Trustwave	ⓘ Suspicious
Abusix	✔ Clean
Acronis	✔ Clean
ADMINUSLabs	✔ Clean
AILabs (MONITORAPP)	✔ Clean
AlienVault	✔ Clean
alphaMountain.ai	✔ Clean
Antiy-AVL	✔ Clean
Artists Against 419	✔ Clean
benkow.cc	✔ Clean
BitDefender	✔ Clean
BlockList	✔ Clean
Blueliv	✔ Clean
Certego	✔ Clean
Chong Lua Dao	✔ Clean
CINS Army	✔ Clean
CMC Threat Intelligence	✔ Clean
CRDF	✔ Clean
Criminal IP	✔ Clean
Cyble	✔ Clean
CyRadar	✔ Clean

9/23/25, 9:04 PM

VirusTotal - URL

desenmascara.me	 Clean
DNS8	 Clean
Dr.Web	 Clean
EmergingThreats	 Clean
Emsisoft	 Clean
ESET	 Clean
ESTsecurity	 Clean
Feodo Tracker	 Clean
Fortinet	 Clean
G-Data	 Clean
Google Safebrowsing	 Clean
GreenSnow	 Clean
Heimdal Security	 Clean
IPsum	 Clean
Juniper Networks	 Clean
Lionic	 Clean
Malware0	 Clean
MalwarePatrol	 Clean
malwares.com URL checker	 Clean
OpenPhish	 Clean
Phishing Database	 Clean
Phishtank	 Clean
PREBYTES	 Clean
Quick Heal	 Clean
Quttera	 Clean
Rising	 Clean
Sangfor	 Clean
Scantitan	 Clean
SCUMWARE.org	 Clean
Seclookup	 Clean
securalytics	 Clean
Snort IP sample list	 Clean
Sophos	 Clean
Spam404	 Clean
StopForumSpam	 Clean
Sucuri SiteCheck	 Clean
ThreatHive	 Clean
Threatsourcing	 Clean
URLhaus	 Clean
Viettel Threat Intelligence	 Clean
ViriBack	 Clean

URL Scanning using Cloudflare Radar:

9/23/25, 10:20 PM

secure-bank-login.com | URL Scanner | Cloudflare Radar



Cloudflare Radar



URL Scanner

Scan ID:

[3d54f592-578f-48ef-8a0e-1463ac52a076](#) Finished

Submitted URL:

<https://secure-bank-login.com/>

Report Finished:

Sep 23, 2025, 15:37:12 Unlisted

Error:

DNS resolution failed