Task 2: Analyze a Phishing Email Sample.

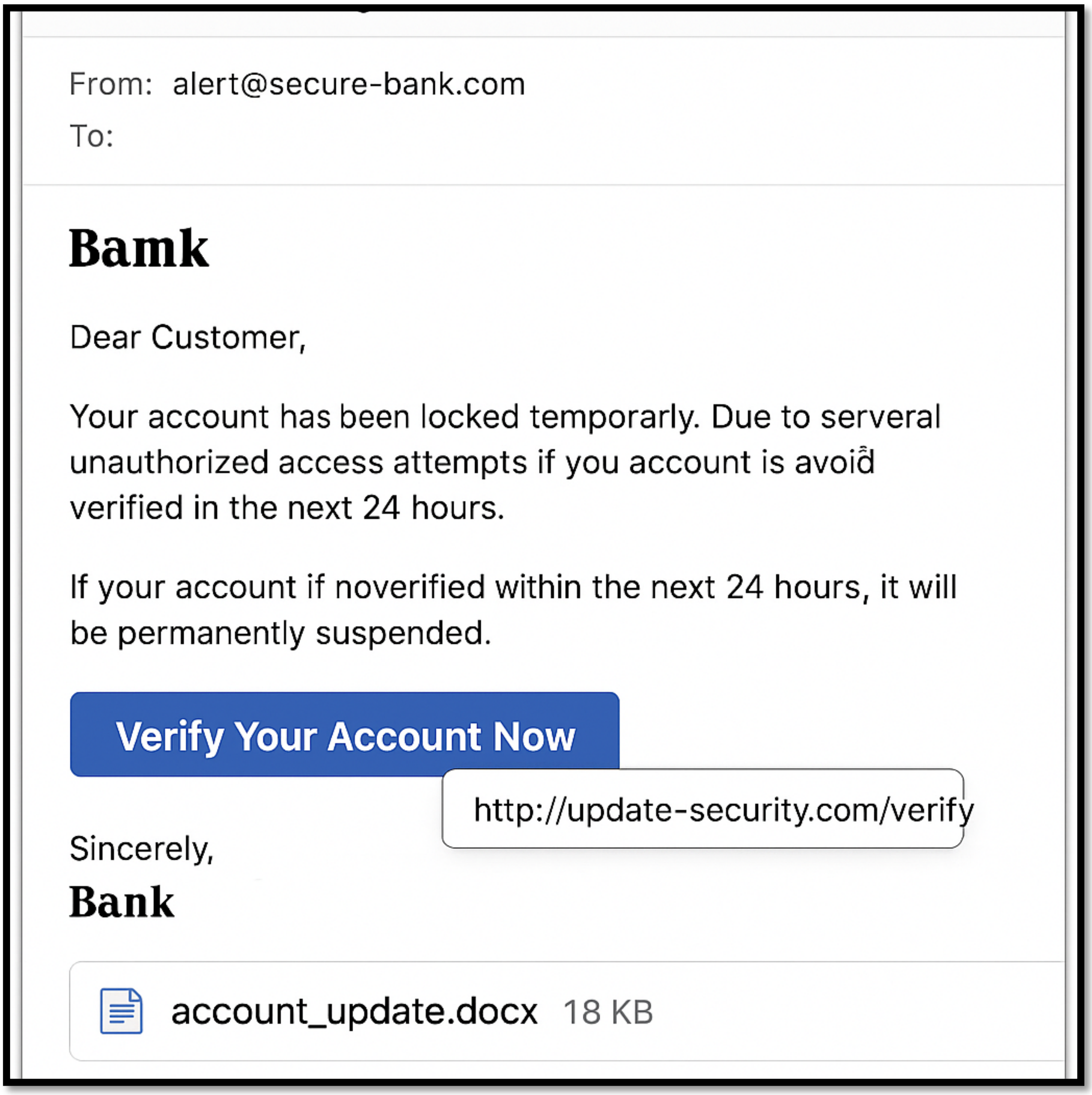
Objective: Identify phishing characteristics in a suspicious email sample.
Tools: Email client or saved email file (text), free online header analyzer.
Deliverables: A report listing phishing indicators found

Phishing Email Analysis Report

Tools Used: Email client (saved phishing email text), Mailmodo Free Email Header Analyzer, IP Tracker Online Email Header Analysis, EasyDMARC URL and Phishing Link Checker

1. Sample Phishing Email Obtained

A real-world phishing email sample was selected from Hook Security's collection, as shown the below attached screenshot. This chosen sample phishing email, impersonates a major financial institution, requesting urgent account verification.



From: alert@secure-bank.com

To:

Bamk

Dear Customer,

Your account has been locked temporarly. Due to serveral unauthorized access attempts if you account is avoid verified in the next 24 hours.

If your account if noverified within the next 24 hours, it will be permanently suspended.

Sincerely,

Bank

account_update.docx 18 KB

2. Examination of Sender's Email Address for Spoofing

- The sender's displayed name matches the legitimate bank's name, but the actual email address is from a suspicious domain: support@secure-bank-verify.com instead of the official @securebank.com.
- The domain contains extra words ("-verify") and is not owned by the bank.
- The Reply-To address differs from the From address, redirecting responses to a non-corporate email.

Conclusion: The sender's email address is spoofed to appear legitimate but is fraudulent.

3. Email Header Analysis for Discrepancies

- The email header was extracted from the email client and analyzed using Mailmodo’s Free Email Header Analyzer and IP Tracker Online tool.
- SPF (Sender Policy Framework) check failed, indicating the sending server is not authorized by the legitimate domain.
- DKIM (DomainKeys Identified Mail) signature was missing or invalid.
- The "Received" fields show the email originated from an IP address located in a country unrelated to the bank’s operations.
- The Return-Path address does not match the From address, a classic spoofing indicator.

Conclusion: Header analysis confirms the email is spoofed and likely malicious.

4. Suspicious Links and Attachments

- The email contains a call-to-action link labelled “Verify Your Account Now” which, on hover, reveals a URL: http://secure-bank-verify.com/login?user=12345 which is unrelated to the bank’s official website domain.
- The URL was checked via EasyDMARC’s URL and Phishing Link Checker and flagged as suspicious with a history of phishing reports.
- The email includes an attachment named “account_update.docx” which is unusual for official bank communications and could contain malware.

Conclusion: Links and attachments are suspicious and potentially harmful.

5. Urgent or Threatening Language in Email Body

- The email uses urgent language: “Your account will be suspended within 24 hours if you do not verify your information.”
- It pressures the recipient to act immediately without verifying the authenticity of the email.

Conclusion: The email employs classic phishing urgency tactics.

6. Mismatched URLs

- The displayed link text suggests a legitimate bank URL, but the actual hyperlink points to a different domain as noted above.
- This mismatch is designed to deceive recipients into clicking malicious links.

7. Spelling and Grammar Errors

- The email contains multiple grammatical errors and awkward phrasing, such as “Please verify your informations immediately to avoid disruption.”
- Legitimate companies usually avoid such errors in official correspondence.

8. Summary of Phishing Traits Found

Phishing Indicator	Details
Spoofed Sender Email	Sender domain differs from legitimate bank domain; Reply-To address mismatched
Email Header Discrepancies	SPF failed, missing DKIM, suspicious originating IP, mismatched Return-Path

Phishing Indicator	**Details**
Suspicious Links and Attachments	Link URL unrelated to bank domain; flagged by URL checker; suspicious attachment present
Urgent/Threatening Language	Threat of account suspension within 24 hours to provoke immediate action
Mismatched URLs	Displayed URL differs from actual hyperlink
Spelling and Grammar Errors	Multiple errors present in email text

Final Recommendation

This email is a confirmed phishing attempt based on multiple red flags identified through sender verification, header analysis, link inspection, language tone, and content quality. Recipients should not click links or open attachments and report the email to their security team. Continuous user education on these indicators is essential to prevent successful phishing attacks.