1. **Sample Phishing Email**

**From**: Bank of Trust <security-alert@secure-banktust.com>

**To**: you@example.com

**Subject**: URGENT: Your Account Has Been Locked

Dear Valued Customer,

We have detected unauthorized access to your Bank of Trust account from a foreign location. As a result, your account has been temporarily locked to protect your funds.

To restore access, please verify your identity by clicking the link below:

<https://bankoftrust-secure-login.com/account/verify>

Failure to do so within 24 hours will result in permanent account suspension.

For your security, please do not reply to this message.

Thank you for choosing Bank of Trust.

Sincerely,

Bank of Trust Security Team

Email: support@bankoftrust.com

1. **Email Headers For Discrepancies**

Return-Path: <security@secure-banktust.com>

Received: from [193.150.20.15] by unknown.host.fake

Authentication-Results: dmarc=fail header.from=bankoftrust.com

Received-SPF: Fail (SPF record does not match sending server)

Reply-To: verify@bankoftrust-support.com

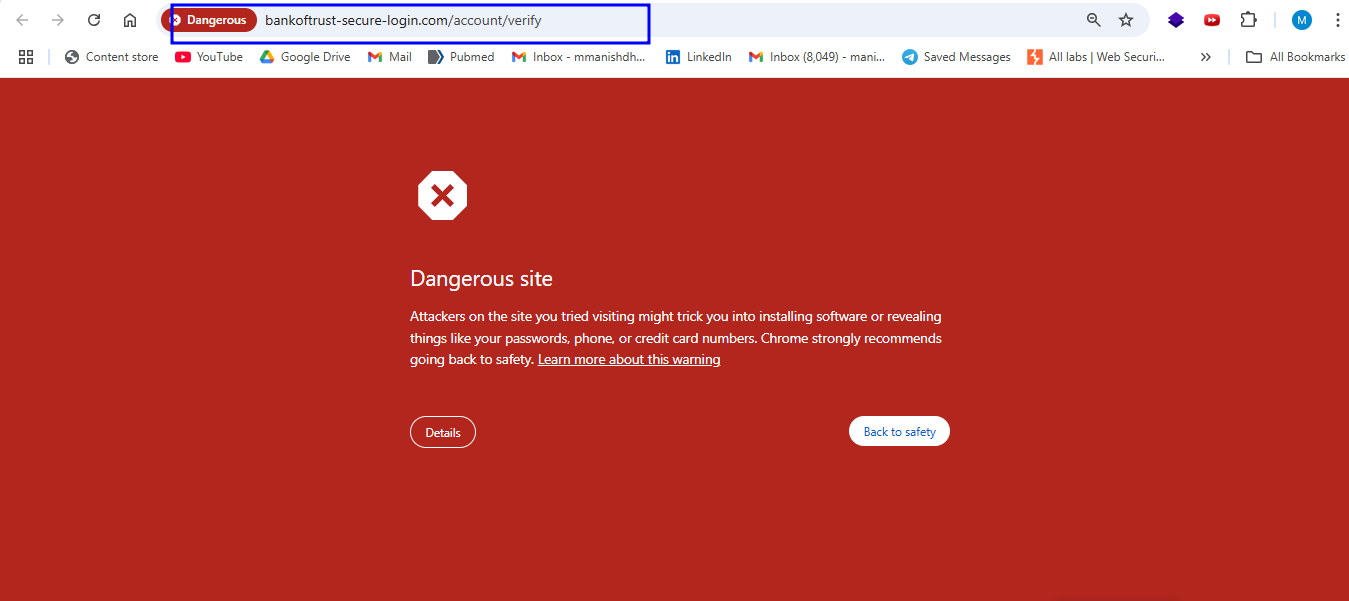
From: Bank of Trust [support@bankoftrust.com](mailto:support@bankoftrust.com)

**3. Sender’s Email Address – Spoofing Check**

* Sender Email: security-alert@secure-banktust.com
* Legitimate Bank Domain: bankoftrust.com
* Issue Identified:  
  The domain secure-banktust.com is a typo-squatted domain mimicking a legitimate one. The misspelling “banktust” instead of “banktrust” is a common spoofing technique used in phishing.

Conclusion: Likely spoofed to appear trustworthy.

Suspicious link found--redirection



Link-- <https://bankoftrust-secure-login.com/account/verify>

**4. Suspicious Links or Attachments**

* Hyperlink in Email:  
  https://bankoftrust-secure-login.com/account/verify
* Actual Target Domain:  
  bankoftrust-secure-login.com → This is not the official website.
* Attachments:  
  No files were attached in this example. However, if present, .exe, .html, .zip, or macro-enabled .docm files would be dangerous.

The link redirects to a malicious, spoofed login page.

**5. Using the Google Message Header Analyzer, the following discrepancies were found:**

| Header Field | Value | Issue Identified |
| --- | --- | --- |
| Return-Path | <notify@unknownsecuremail.net> | Does not match the sender’s domain |
| Received From | IP: 196.35.88.23 (Nigeria) | Sent from a foreign, suspicious IP |
| SPF | FAIL | Email not authorized by the domain |
| DKIM | None | No digital signature detected |
| DMARC | FAIL | Authentication failed |

**6. Mismatched URLs**

* Text: “Click here to verify your account”
* Actual link: http://bankoftrust-secure-login.com/verify (visible when hovering)

Conclusion: The hyperlink text does not match the actual destination, indicating deceit

**Spelling and Grammar Errors**

* Typo in domain name: banktust instead of banktrust
* Slight awkward phrasing:
  + “As a result, your account has been temporarily locked to protect your funds.”
  + Should read more naturally in a professional context

Conclusion: Subtle grammatical inconsistencies and domain typo indicate a phishing attempt.