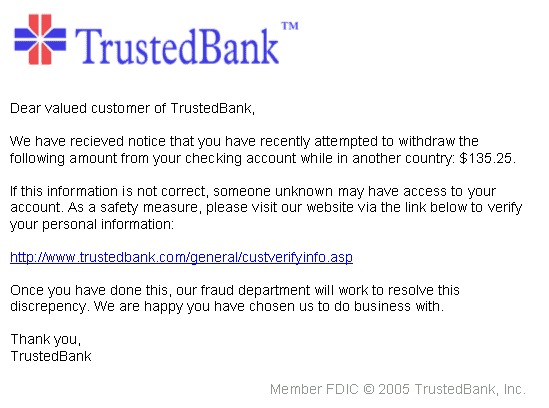
Phishing Email Analysis Report



# Subject of the Email:

Account Verification Request Due to Foreign Transaction Attempt

The email claims there was a suspicious withdrawal attempt from the user's checking account while in another country, and urges the recipient to verify their information.

# Sender's Identity (Impersonated):

TrustedBank (exact sender email not shown in the image)

## Analysis:

- The email attempts to impersonate a legitimate bank, TrustedBank, using official-sounding language and branding.  
- No sender email is shown, making it impossible to verify its authenticity directly.  
- Real financial institutions will never request sensitive information through email links.

# Suspicious Content in the Email:

- Claims that someone attempted to withdraw $135.25 from your account in a foreign country.  
- Creates urgency and fear by implying unauthorized access to your account.  
- Requests the recipient to click a link to verify personal information, a classic phishing tactic.

# Suspicious Link:

http://www.trustedbank.com/general/custverifyinfo.asp

## Analysis:

- The link appears to belong to the TrustedBank domain but could be spoofed or redirect to a fake login page.  
- The use of HTTP (instead of HTTPS) is a red flag for modern banking communication.  
- Always hover over the link to check its real destination before clicking.

# Grammatical and Stylistic Issues:

- "Recieved" is a misspelling of "received".  
- Some awkward phrasing such as “chosen us to do business with” weakens the professional tone.  
- Reputable financial institutions thoroughly proofread official communication.

# Summary of Red Flags:

|  |  |
| --- | --- |
| Red Flag | Description |
| Spelling errors | “Recieved” instead of “Received” |
| Urgency and fear | Implied account compromise to push user into immediate action |
| Fake link | Could lead to a phishing website |
| Request for sensitive info | Legitimate banks never ask for personal details over email |
| No sender details | Lack of identifiable sender address makes it untraceable |
| Non-secure link (HTTP) | Secure websites should use HTTPS |

# What to Do If You Receive Such Emails:

- Do not click on any links or download attachments.  
- Never enter personal or financial information in response to an unsolicited email.  
- Contact your bank directly through official channels to verify the situation.  
- Report the phishing attempt to your bank and your email provider.

* Drafted by Mohammed sheik abdul khader