Report on Email Analysis

Red Flags Struck:

1. **Use of Fear and Urgency:** The email uses fear and urgency to get the reader to act right now.

2. **Generic Greeting:** A generic greeting ("Dear Customer") at the beginning of the email suggests that it is not personalized.

3. **Suspicious Links:** When a link is looked over, it is shown that it does not correspond to the sender's legitimate website(**securebank.com**).

4. **Unexpected Attachment:** The email contains an unexpected attachment called "**AccountDetails.zip**," which may be a malicious file.

5. **Unusual Sender Address:** Even if the sender address seems legal, it's crucial to properly check the sender's legitimacy.

How to Prevent These Attacks:

1. **Check the Sender:** Always verify that the email address being sent matches the organization's official domain by checking it twice. Watch out for minor spelling or variation errors.

2. **Steer clear of urgent requests:** Be wary of emails that encourage you to take immediate action. Before sharing any sensitive information, take your time to carefully review the request.

Report on Email Analysis

3 **How ever your Mouse Over Links To Preview The URL:** Hover Your Mouse Over Any Links In The Email. Avoid clicking on any links that take you to shady or unexpected websites.

4 **Avoid Opening Surprising Attachments:** Avoid accessing attachments from unidentified or unexpected sources. 4. Do Not Open Unexpected Attachments. Before downloading or opening any files, verify with the sender if you have any doubts.

5 Use two-factor authentication: Make sure your email and other accounts have two-factor authentication enabled. Even if your password is stolen, this adds an extra degree of security.

6Employees: It's critical for businesses to educate staff **Educate** members on email security, spotting phishing scams, and adhering to correct procedures for request verification

7**Install Reliable Security Software:** To identify and stop unwanted software from infecting your system, use reliable antivirus and anti-malware software.
You may dramatically lower your chance of falling for phishing scams by being watchful, confirming the legitimacy of emails, and adhering to recommended practices for email security.
Please note that this analysis is a fictional example that i have made, and real-life situations may vary. Always exercise caution and follow best practices to stay safe online.