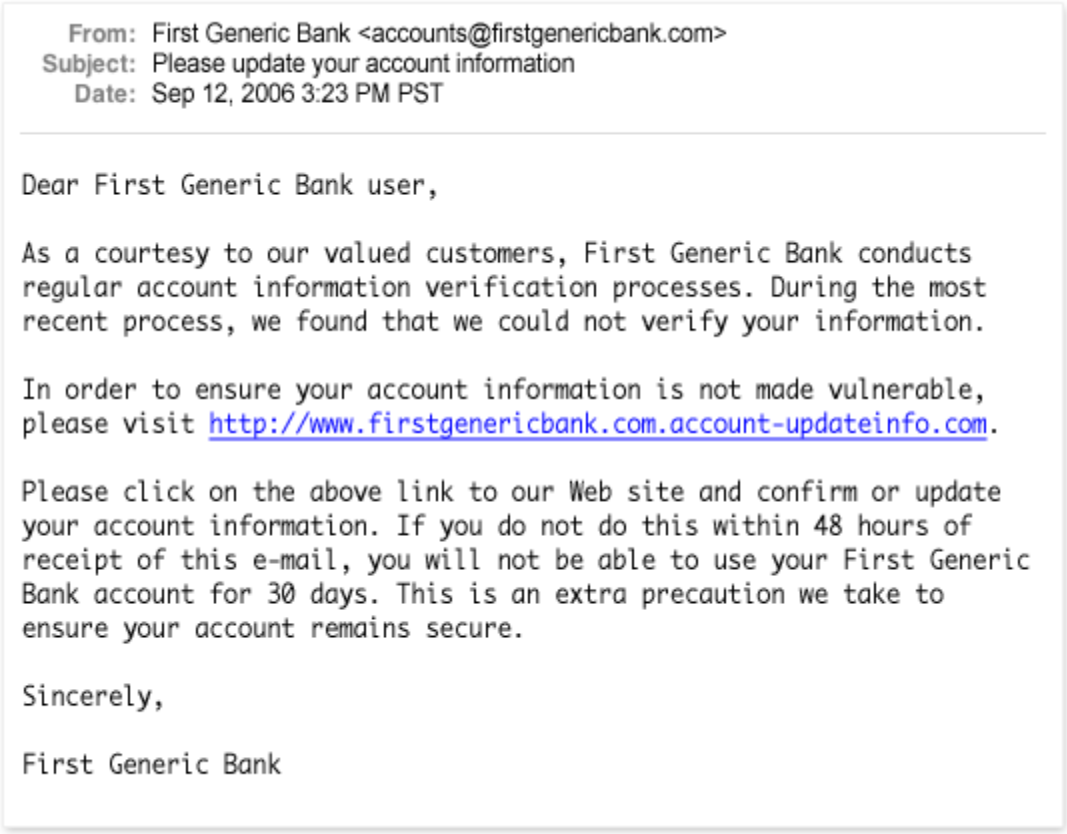
TASK -2 : Analyse a Phishing Email Sample.

Objective: Identify phishing characteristics in a suspicious email sample.

Tools: Email client or saved email file (text), free online header analyser.

Deliverables: A report listing phishing indicators found

SAMPLE PHISHING EMAIL ADRESS - **Phishing Email Analysis Report**



From: First Generic Bank <accounts@firstgenericbank.com>
Subject: Please update your account information
Date: Sep 12, 2006 3:23 PM PST

Dear First Generic Bank user,

As a courtesy to our valued customers, First Generic Bank conducts regular account information verification processes. During the most recent process, we found that we could not verify your information.

In order to ensure your account information is not made vulnerable, please visit http://www.firstgenericbank.com.account-updateinfo.com.

Please click on the above link to our Web site and confirm or update your account information. If you do not do this within 48 hours of receipt of this e-mail, you will not be able to use your First Generic Bank account for 30 days. This is an extra precaution we take to ensure your account remains secure.

Sincerely,

First Generic Bank

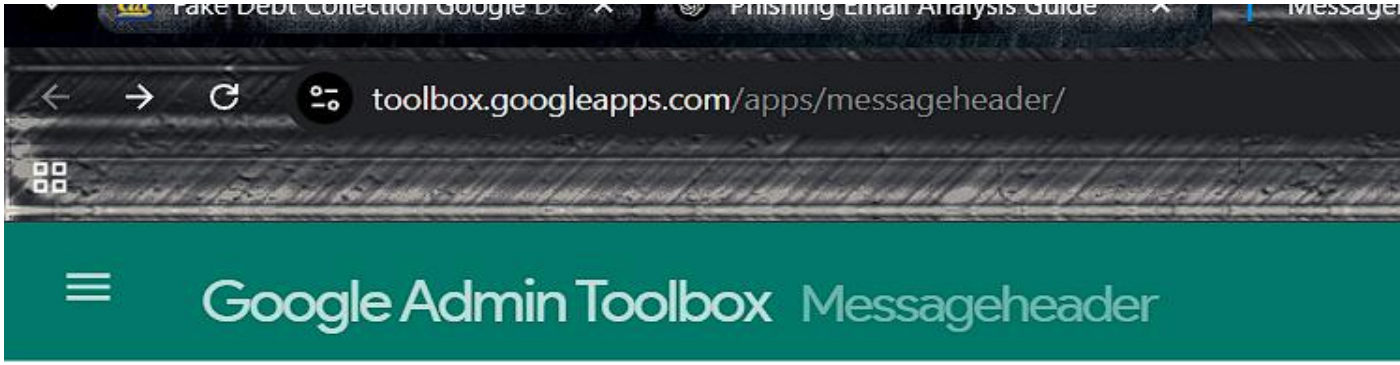
Email Details:

- **From:** accounts@firstgenericbank.com
- **Subject:** Please update your account information
- **Date:** Sep 12, 2006, 3:23 PM PST
- **Greeting:** "Dear First Generic Bank user" (Generic)

Suspicious things identified.

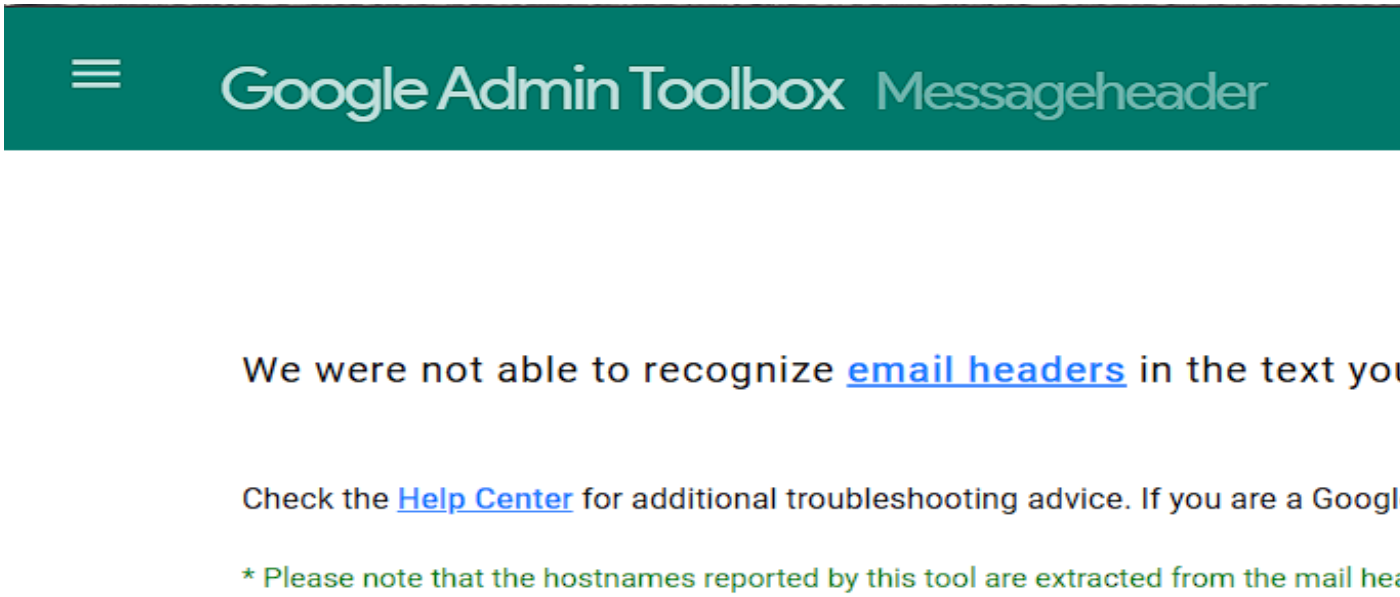
Appears **to be from:** accounts@firstgenericbank.com

But phishing attackers can **forge the "From" field**.



accounts@firstgenericbank.com

ANALYZE THE HEADER ABOVE



Suspicious URL

- **Displayed Link:** http://www.firstgenericbank.com.account-updateinfo.com
- **Issue:** It **mimics a legitimate domain** but is actually a **malicious domain**:
    - Real domains don't start with other domain names.
    - This URL belongs to account-updateinfo.com, not firstgenericbank.com.

Generic Salutation

- **Says:** "Dear First Generic Bank user"
- Legitimate banks typically address users by **full name** for personalization.
- **Generic greeting = mass phishing attempt.**

Trait	Observation
Spoofed Sender	Likely forged sender name & email
Suspicious URL	Link belongs to fake domain, not the bank
Urgent Language	Threat of account suspension in 48 hours
Generic Greeting	"Dear user" instead of real name

Misleading Purpose	Poses as a security verification
Lack of Contact Details	No phone or verifiable bank contact info

1. What is phishing?

Phishing is a type of cyberattack where attackers impersonate legitimate organizations or individuals to trick users into revealing sensitive information like passwords, financial details, or personal data. It typically occurs via fraudulent emails, messages, or websites designed to appear trustworthy.

2. How to identify a phishing email?

Phishing emails often contain the following traits:

- Generic greetings like “Dear Customer” instead of your real name.
- Urgent or threatening language demanding quick action.
- Suspicious email addresses (spoofed or slightly misspelled).
- Links that don’t match legitimate domains (hover to preview).
- Requests for sensitive data like passwords or credit card details.
- Spelling or grammatical errors.
- Attachments with suspicious extensions (.exe, .scr, .docm).

3. What is email spoofing?

Email spoofing is when an attacker forges the “From” address in an email to make it appear as though it's from a trusted source. This tricks users into believing the message is authentic, often as part of phishing or spam attacks. The spoofed email doesn’t actually originate from the stated address.

4. Why are phishing emails dangerous?

Phishing emails are dangerous because:

- They can steal credentials and financial data.
- They may install malware or ransomware on your system.
- They can lead to identity theft or unauthorized access to systems.

- They can exploit human trust using social engineering.

5. How can you verify the sender's authenticity?

To verify an email sender:

- Check the full email address, not just the display name.
- Use email header analysis tools to check SPF, DKIM, and DMARC records.
- Cross-verify the sender's domain via WHOIS or public records.
- Look for inconsistencies in domain names or links.

6. What tools can analyze email headers?

Some free tools include:

- Google Admin Toolbox: https://toolbox.googleapps.com/apps/messageheader/
- MXToolbox Email Header Analyzer
- Mailheader.org
- Email forensic tools like GCA Email Threat Analyzer

7. What actions should be taken on suspected phishing emails?

- Do **not** click links or download attachments.
- Report the email to your organization's security team or use "Report Phishing" option.
- Move the email to the spam or junk folder.
- Use sandbox environments for safe analysis.
- Block sender and related domains if confirmed malicious.

8. How do attackers use social engineering in phishing?

Social engineering tricks victims using psychological tactics like:

- Urgency ("Update now or lose access!")
- Authority (posing as a CEO, bank, or IT admin)

- Curiosity (fake invoices or alerts)
- Fear (threat of account closure or fines)

These are used to bypass technical defenses and exploit human trust or panic.