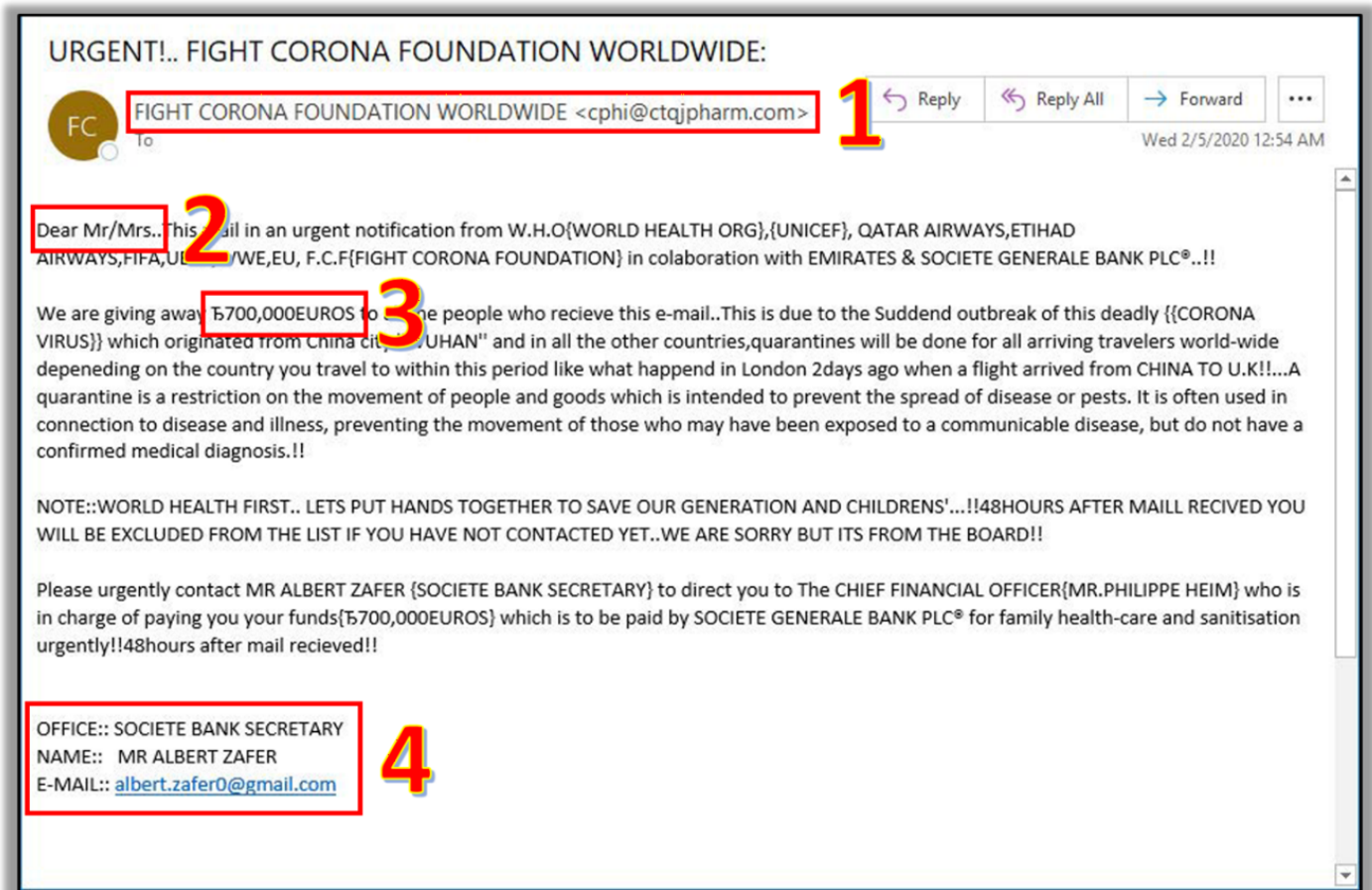


Identifying Phishing



1. Suspicious Senders

- Always Check the Sender's email address
- Look for subtle misspellings or unusual domain names

2. Generic Greetings

- Be cautious of generic greetings
- Phishing emails often use greetings like "Dear Customer" instead of your actual name

3. Urgent or Threatening Language

- Beware of emails that create a sense of urgency or fear
- Phrases like

“Your account will be suspended,”

“Immediate action required,” or

“URGENT”

- May also promise rewards of some kind

4. Mismatched URLs

WATCH OUT FOR...

From: Security Bank (accounts.securitybank@gmail.com)
Subject: Action Required!

Dear valued customer,

You are require to update your account information immediately to prevent account termination. Please follow link to update password information and verify your email address:

www.securitybank.net/info
<http://www.malware.com/hack.php>

Please be sure to read the updated privacy policies in the attached document.

Thanks,
 Security Bank Account

[privacypdf.exe](#)

Annotations:

- a sense of urgency (points to "Action Required!")
- an illegitimate or unfamiliar address (points to "accounts.securitybank@gmail.com")
- a generic greeting or salutation (points to "Dear valued customer,")
- spelling & grammar mistakes (points to "You are require")
- suspicious links or links that don't match the destination (points to "http://www.malware.com/hack.php")
- unexpected attachments (especially files ending in .exe) (points to "privacypdf.exe")

Poor

Grammar and Spelling

- Look for spelling and grammatical errors

- Phishing emails often contain typos and awkward phrasing
- This is often due to attackers using Google Translate to translate into English

Unexpected Attachments or Links

- Do not open unexpected attachments or click on suspicious links
- A link might say 'www.yourbank.com' but actually lead to a different website
- Do not open an attachment if it is a `.exe` (Windows) or `.dmg` (MacOS)

Request for Personal Information

- Legitimate organizations will not ask for sensitive information via email
 - Emails asking for passwords, Social Security numbers, or credit card details are likely phishing attempts
-
-

Revision #6

Created 2025-06-20 13:15:21 UTC by Jefferson Davis

Updated 2026-04-28 18:56:13 UTC by Jefferson Davis