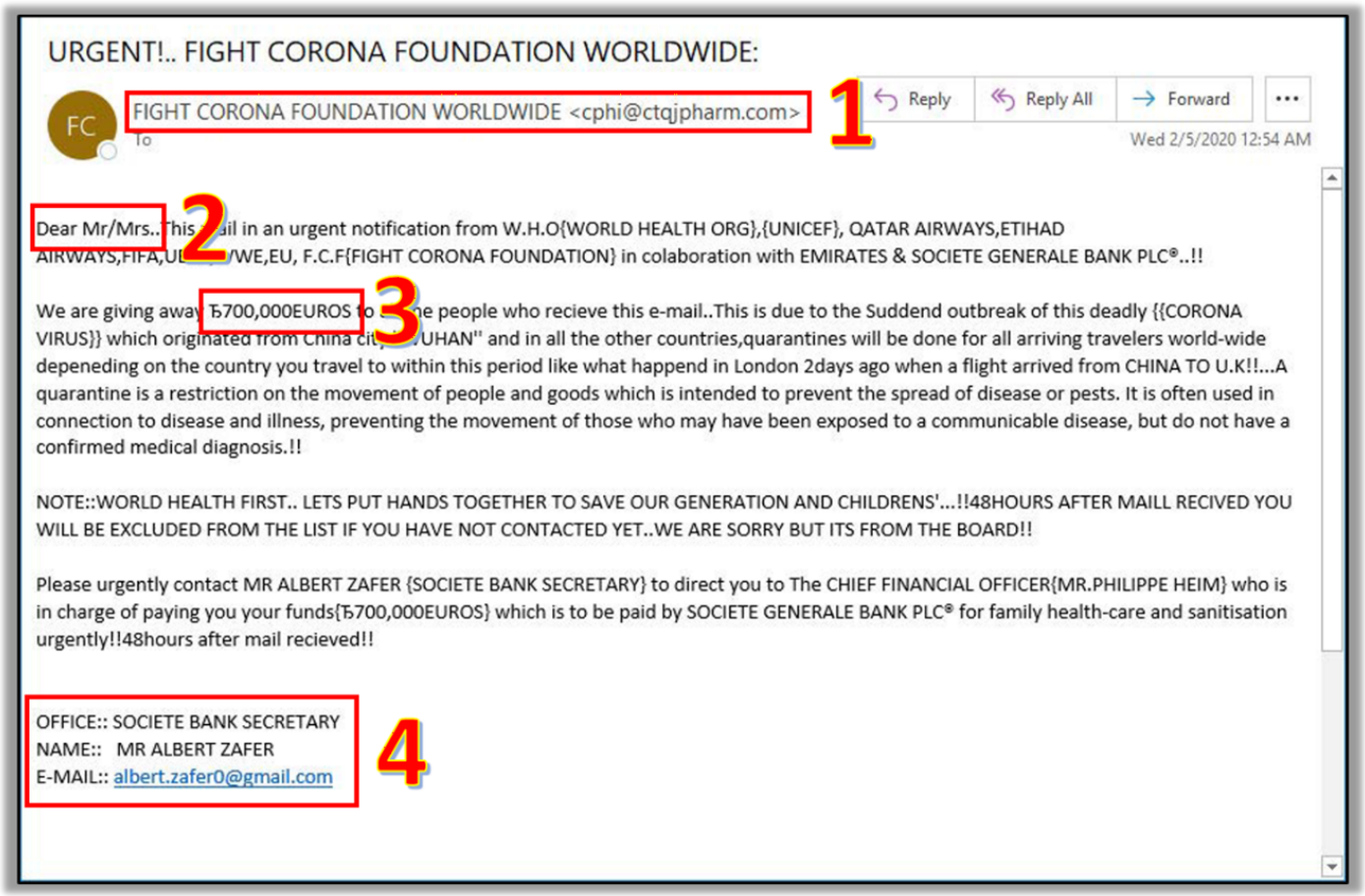
Identifying Phishing



1. Suspicious Senders

- 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

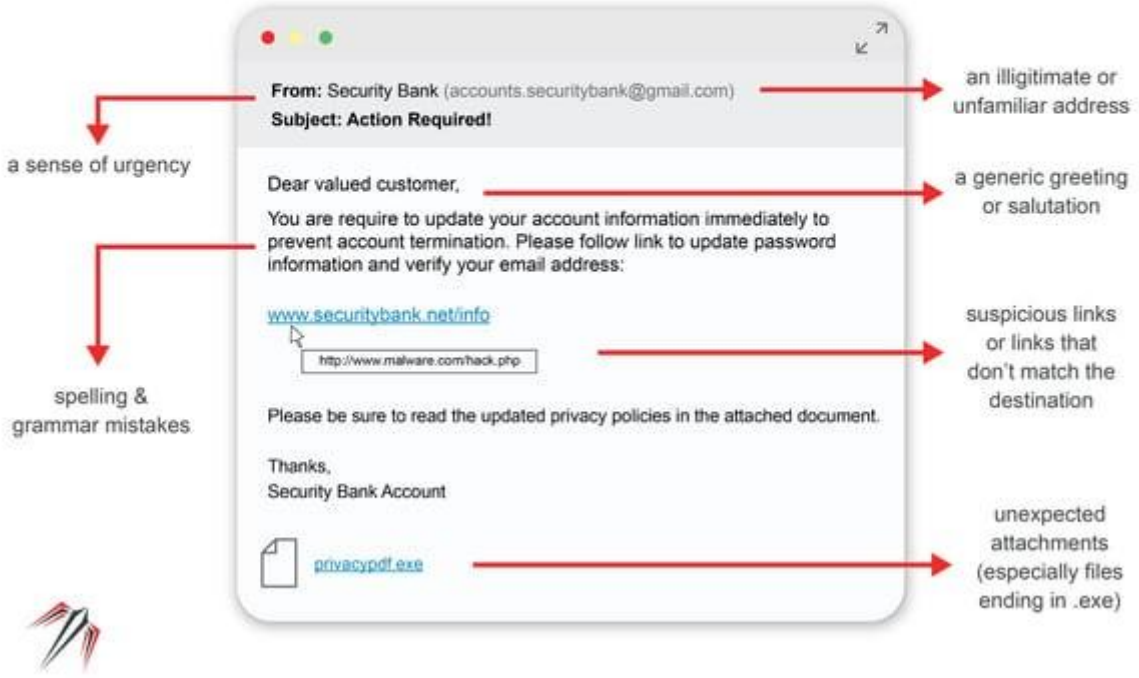
- Beware of emails that create a sense of urgency or fear
- Phrases like

> “Your account will be suspended,”
>
> “Immediate action required,” or
>
> “URGENT”

- May also promise rewards of some kind

4. Mismatched URLs

- Ensure the URLs in the email match the legitimate website
- Hover over links to see the actual URL



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

If you Suspect an email is Phishing

If you suspect that an email is a phishing attempt, please refer to Handling Suspicious Emails and follow the instructions to report the email to the IT Department.

Revision #3
Created 2025-06-20 13:22:49 UTC by Jefferson Davis
Updated 2026-04-20 19:17:30 UTC by Jefferson Davis