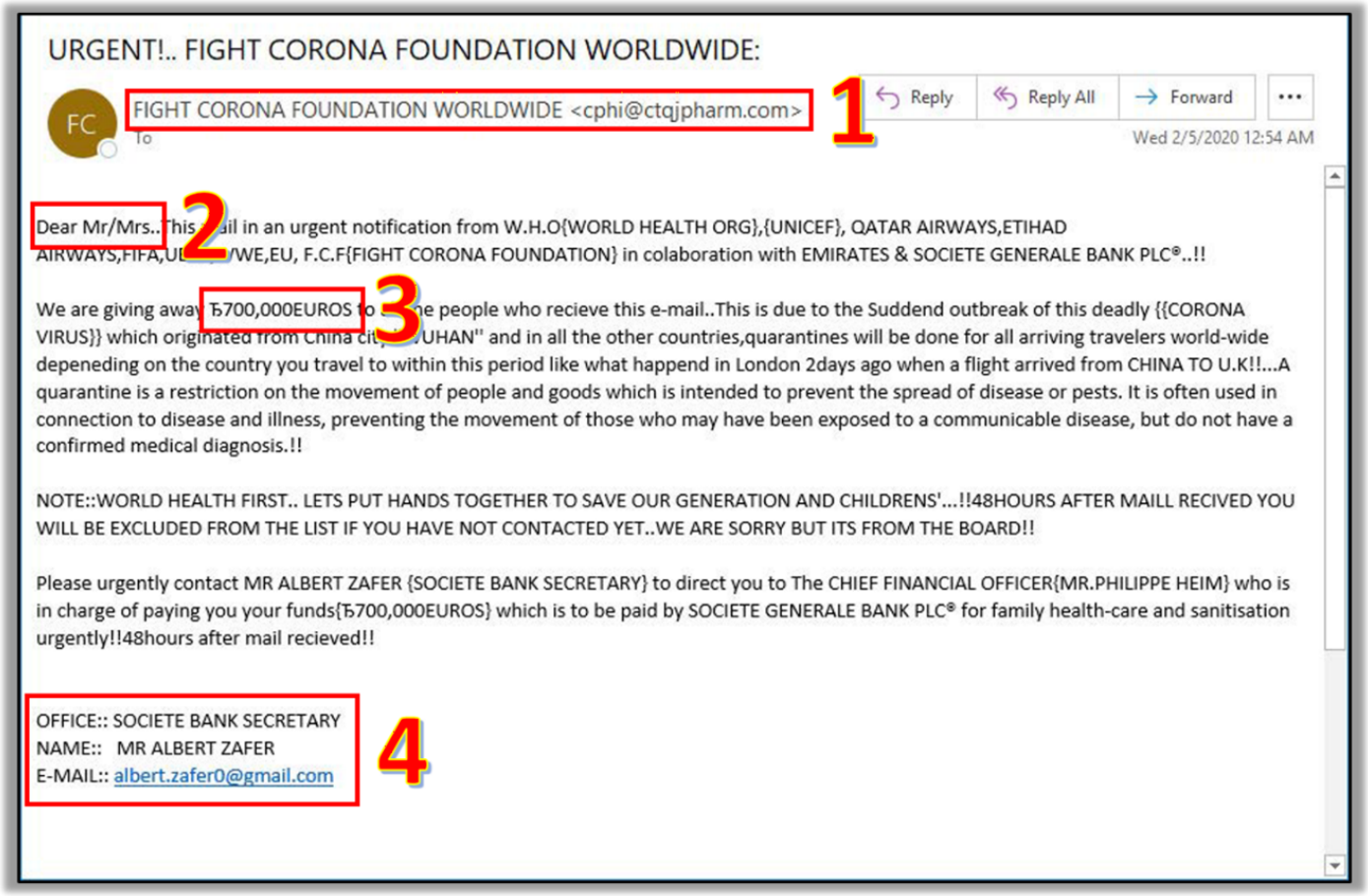
Identify Phishing Emails

> *Phishing emails are malicious attempts to obtain sensitive information such as usernames, passwords, and credit card details by disguising themselves as trustworthy entities. This guide will help you identify phishing emails and protect your personal information.*



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 like "Dear Customer" instead of your actual name.

---

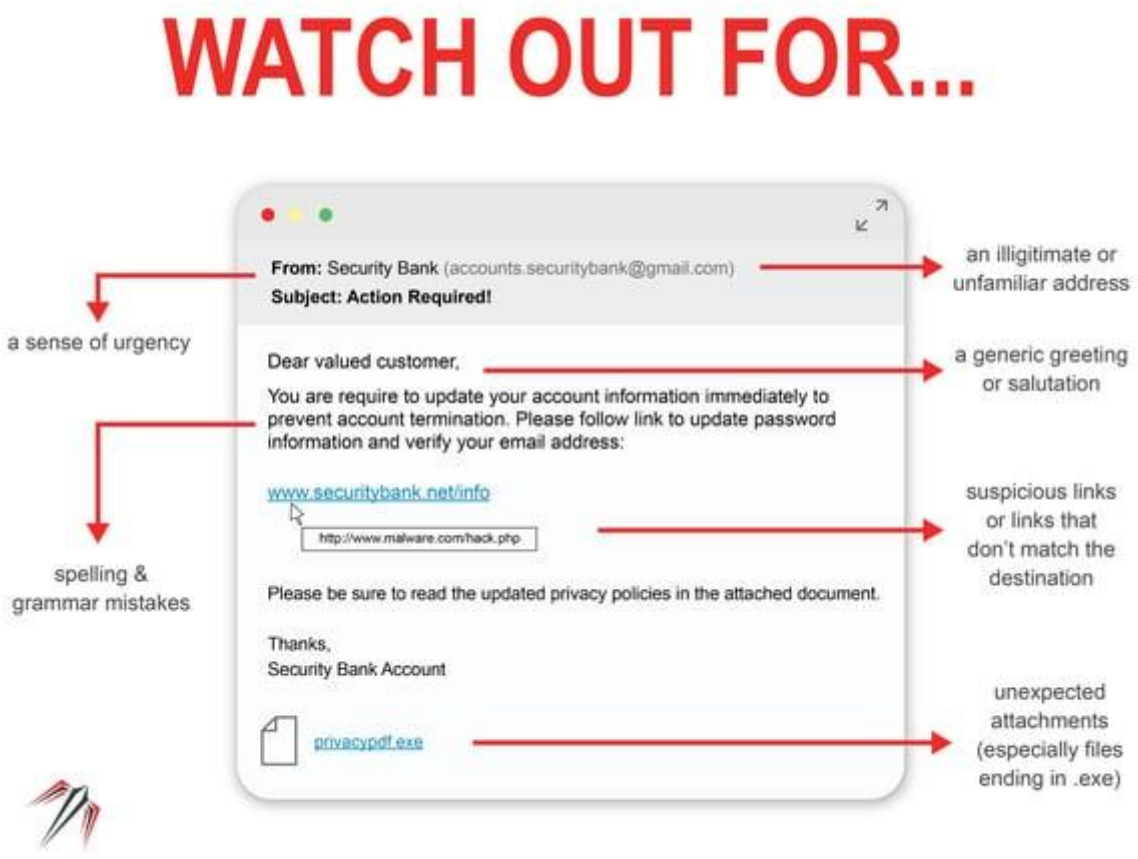
3. Urgent or Threatening Language

- Beware of emails that create a sense of urgency or fear.
  - Phrases like "Your account will be suspended," or "Immediate action required" or "URGENT"
  - Phishing emails may also promise rewards of some kind.

---

4. Mismatched URLs

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



5. 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 to English.

6. Unexpected Attachments or Links

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

7. Request for Personal Information

- Legitimate organizations generally do not ask for sensitive information via email.
  - Emails asking for passwords, social security numbers, or credit card details are likely phishing attempts.

Revision #3
Created 2025-10-21 18:29:36 UTC by Jefferson Davis
Updated 2026-04-28 19:02:22 UTC by Jefferson Davis