Suspicous Emails (Phishing)

This guide provides clear, step-by-step instructions for identifying and reporting phishing emails using Microsoft Outlook (2016, 2024, and Outlook Web App). It outlines the proper use of the built-in reporting tools, explains how to safely handle suspicious messages, and offers best practices to protect yourself and the university from email-based threats.

Handling Suspicious Emails

> **“I think I’ve received a Phishing email! What should I do?!”**

Do not click on Links or open Attachments

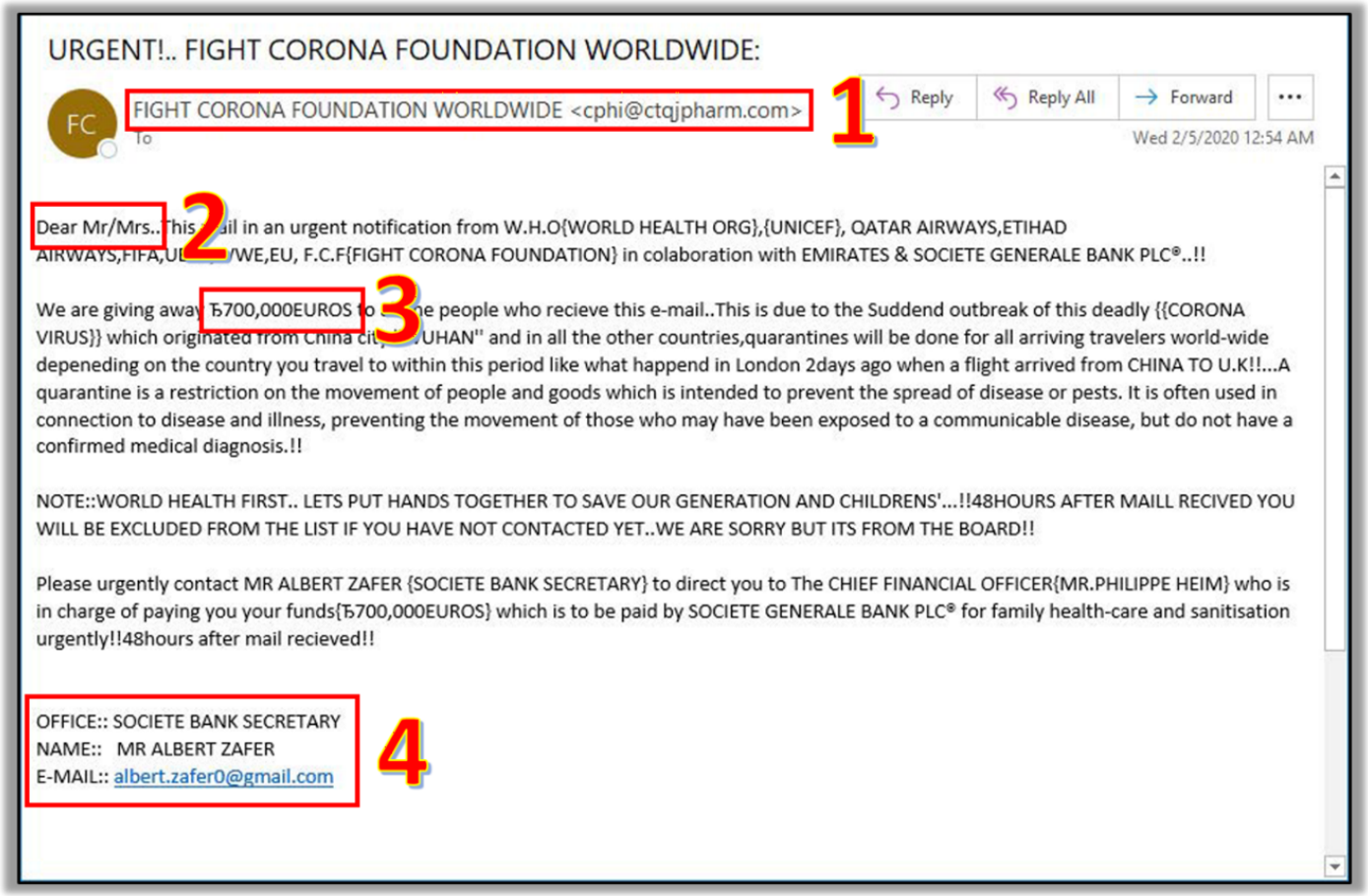
Avoid Interacting with any content in the email

Verify the Sender

Use the Report Phishing button in Outlook to report phishing emails to the IT Department

Remove the phishing email from your inbox and trash folders after reporting it to IT

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

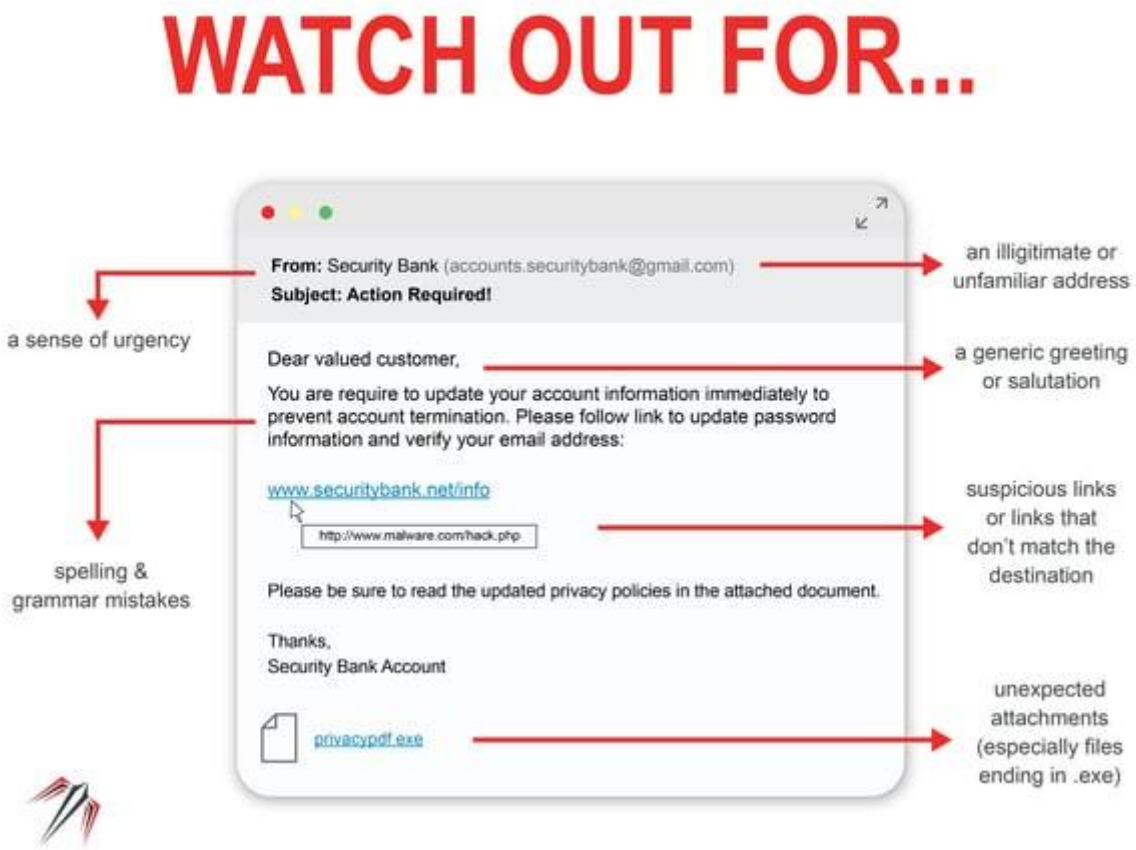
3. Urgent or Threatening Language

- 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



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)

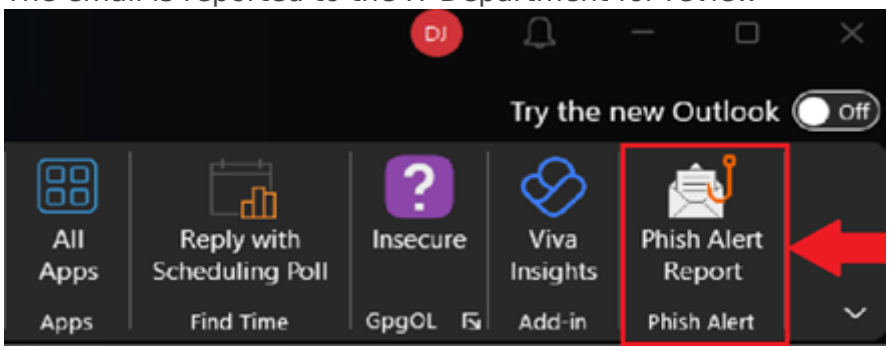
Request for Personal Information

- 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

---

Outlook (Classic)

1. Navigate to **Inbox**
2. Select the email you wish to report, and ensure the email is highlighted
3. Under the **Home** tab, In the far-right corner, select **Phish Alert Report**
4. The email is reported to the IT Department for review



Outlook (New)

1. Navigate to **Inbox**
2. Select the email you wish to report, and ensure the email is highlighted
3. Select the **Home** tab
4. Use the **Report** button (located next to Reply) to report the email
5. A popup will appear asking if you're sure you'd like to report the email. Select **Report**
6. The email is reported to the IT Department for review
7. These instructions also apply to **Outlook Web Online (OWA)**