

# Phishing

- [Identify Phishing Emails](#)
- [Report Phishing Emails](#)

# 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.

The screenshot shows an email interface with the following elements highlighted:

- 1**: The sender's name and email address: "FIGHT CORONA FOUNDATION WORLDWIDE <cphi@ctqjpharm.com>".
- 2**: The greeting: "Dear Mr./Mrs..".
- 3**: A monetary amount: "€700,000EUROS".
- 4**: A contact information block: "OFFICE:: SOCIETE BANK SECRETARY", "NAME:: MR ALBERT ZAFER", "E-MAIL:: [albert.zafer0@gmail.com](mailto:albert.zafer0@gmail.com)".

The email body text includes: "URGENT!.. FIGHT CORONA FOUNDATION WORLDWIDE:", "Dear Mr./Mrs.. This mail in an urgent notification from W.H.O{WORLD HEALTH ORG},{UNICEF}, QATAR AIRWAYS,ETIHAD AIRWAYS,FIFA,UEFA,WE,EU, F.C.F{FIGHT CORONA FOUNDATION} in collaboration with EMIRATES & SOCIETE GENERALE BANK PLC®..!!", "We are giving away €700,000EUROS to some people who recieve this e-mail..This is due to the Sudden outbreak of this deadly {{CORONA VIRUS}} which originated from China city of "WUHAN" and in all the other countries,quarantines will be done for all arriving travelers world-wide depeneding on the country you travel to within this period like what happend in London 2days ago when a flight arrived from CHINA TO U.K!!...A quarantine is a restriction on the movement of people and goods which is intended to prevent the spread of disease or pests. It is often used in connection to disease and illness, preventing the movement of those who may have been exposed to a communicable disease, but do not have a confirmed medical diagnosis.!!", "NOTE::WORLD HEALTH FIRST.. LETS PUT HANDS TOGETHER TO SAVE OUR GENERATION AND CHILDRENS'...!!48HOURS AFTER MAILL RECIVED YOU WILL BE EXCLUDED FROM THE LIST IF YOU HAVE NOT CONTACTED YET..WE ARE SORRY BUT ITS FROM THE BOARD!!", "Please urgently contact MR ALBERT ZAFER {SOCIETE BANK SECRETARY} to direct you to The CHIEF FINANCIAL OFFICER{MR.PHILIPPE HEIM} who is in charge of paying you your funds{€700,000EUROS} which is to be paid by SOCIETE GENERALE BANK PLC® for family health-care and sanitisation urgently!!48hours after mail recieved!!".

## 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.

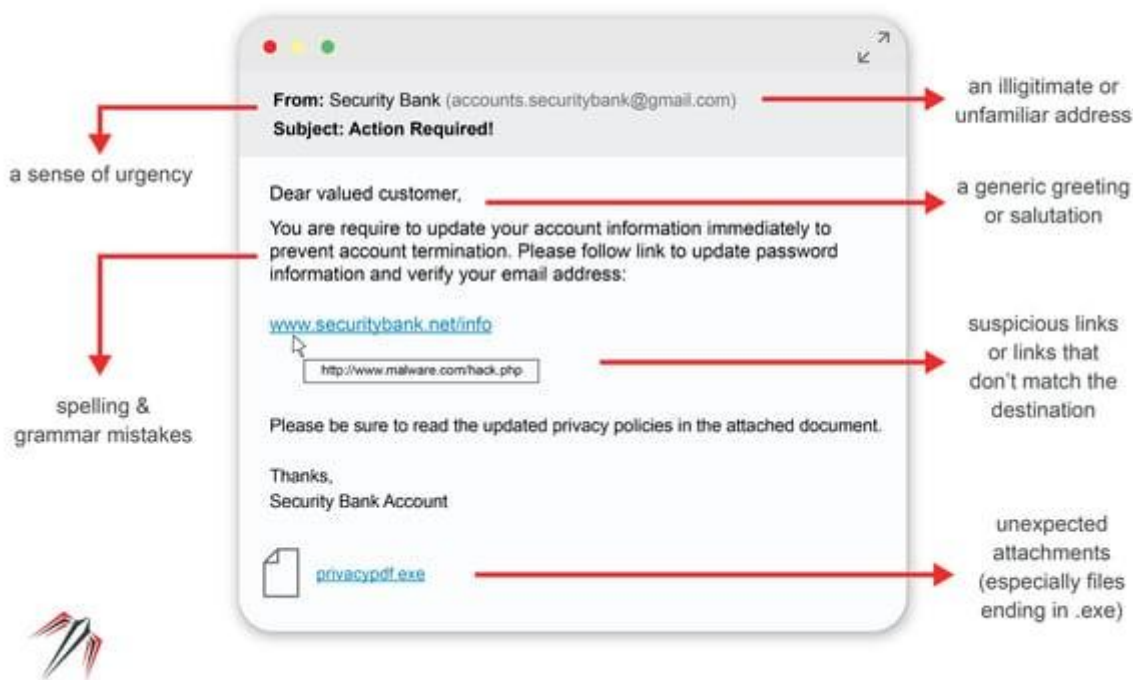
## 3. Urgent or Threatening Language

- 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.
- 

# WATCH OUT FOR...



## 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.
-

# Report Phishing Emails

**I think I've received a Phishing email! What should I do!?"**

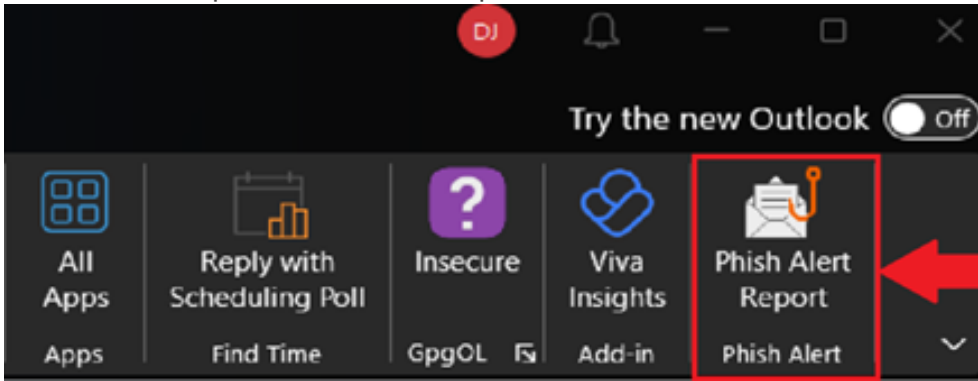
- Do not click on links or open attachments
  - Avoid interacting with any content in the email
- Verify the Sender
  - Contact the organization directly using official contact details that are not provided in the email.
- Report the Email
  - Use the Report Phishing button in Outlook to Report phishing emails to the IT Department.
- Delete the Email
  - Remove the phishing email from your inbox and trash folders after reporting it to IT.

## Report Phishing (Outlook Classic)

You must report a Phishing email using a PC or Mac

- Navigate to **Inbox**
- Select the email you wish to report, and ensure the email is highlighted.
- Under the **Home** tab, in the far-right corner, select **Phish Alert Report**

- The email is reported to the IT Department for review.



## Report Phishing (Outlook New)

These instructions also work for the Outlook Web Application (OWA)

- Navigate to **Inbox**
- Select the email you wish to report, and ensure the email is highlighted.
- Select the **Home** tab
- Use the **Report** button (Located next to **Reply**) to report the email.
- A popup will appear asking if you're sure you'd like to report the email. Select **Report**.
- The email is reported to the IT Department for review

