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

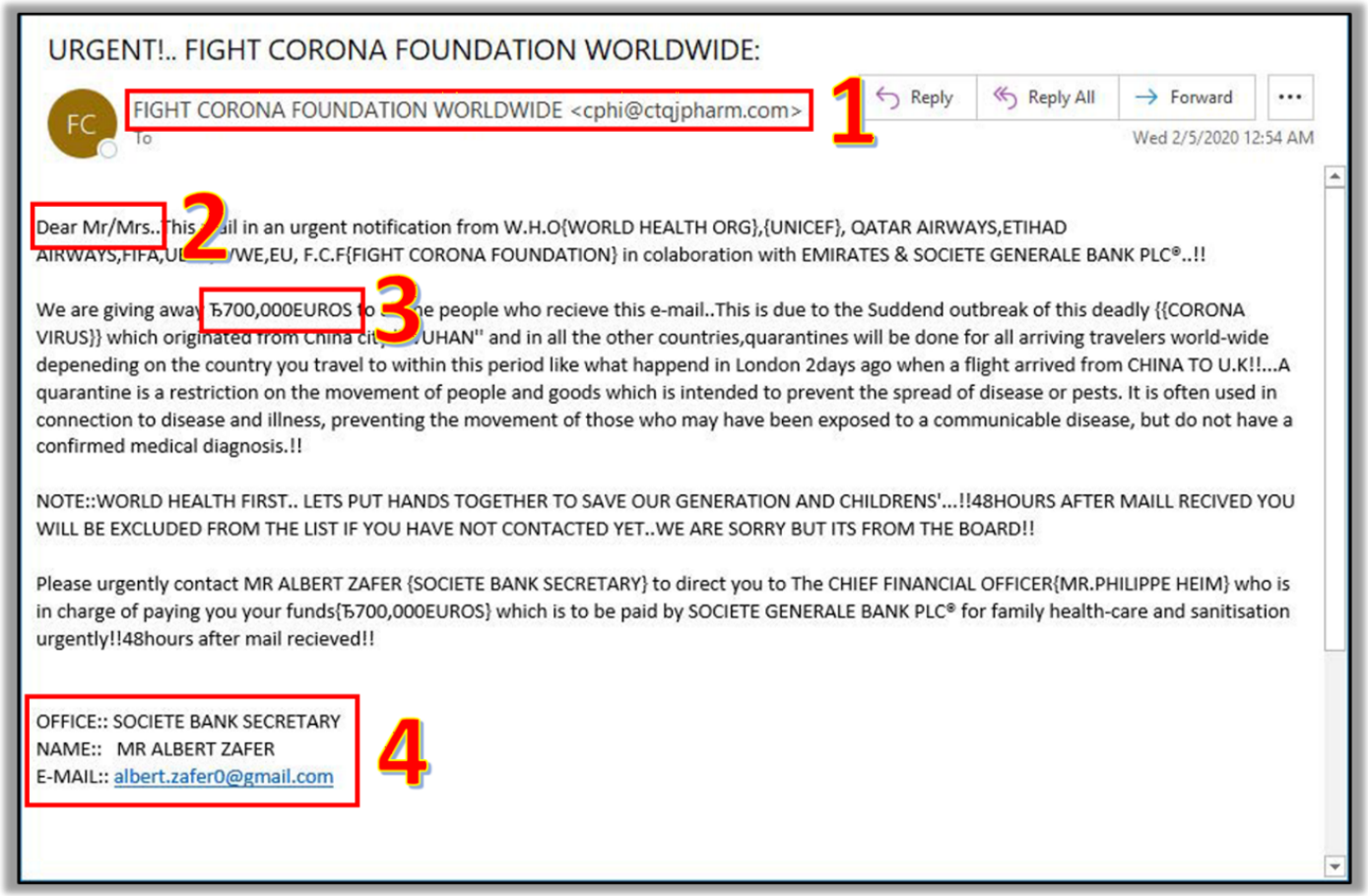
Avoid Interacting with any content in the email

Verify the Sender

Use the Report Phishing button in Outlook to report phishing emails to the IT Department Outlook (New) Click this link to view instructions

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

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

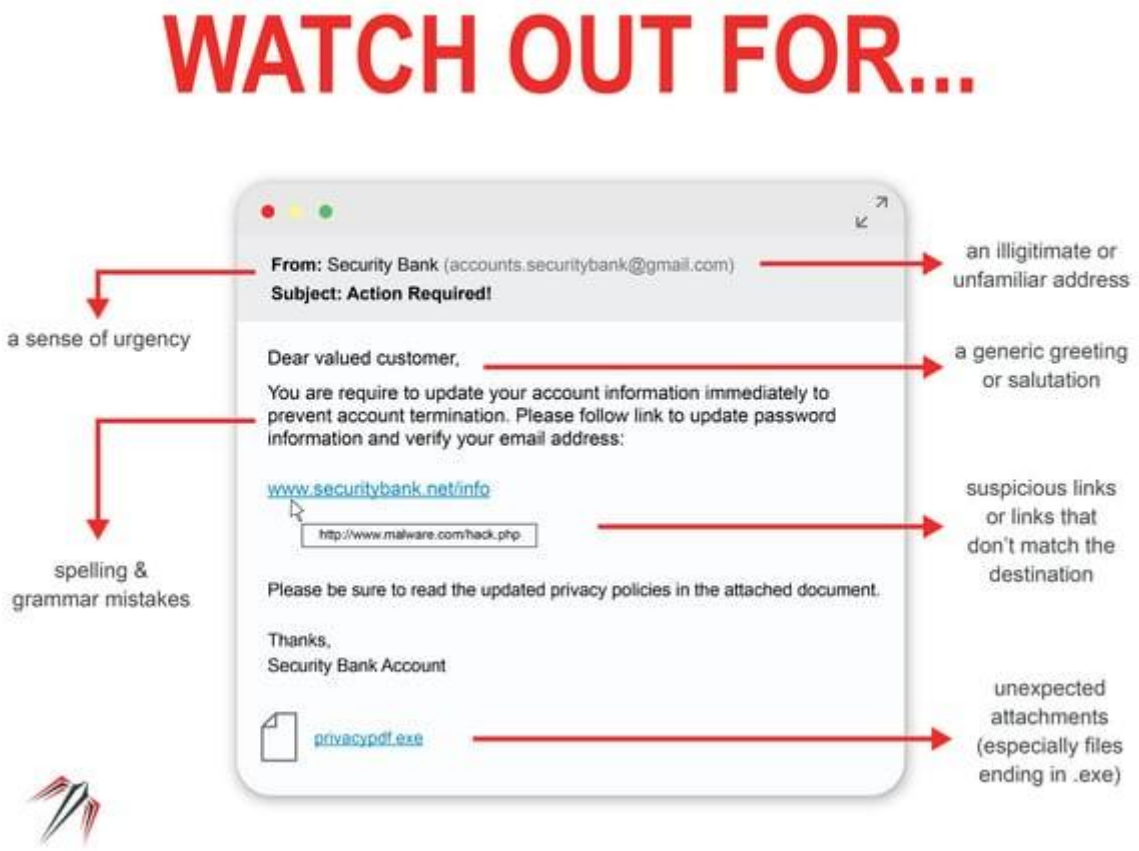
- Beware of emails that create a sense of urgency or fear

- Phrases like

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

- May also promise rewards of some kind

4. Mismatched URLs



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

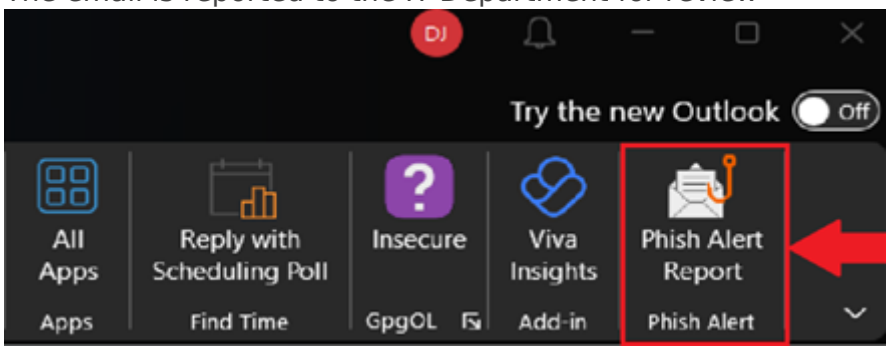
- Legitimate organizations will not ask for sensitive information via email
- Emails asking for passwords, Social Security numbers, or credit card details are likely phishing attempts

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.

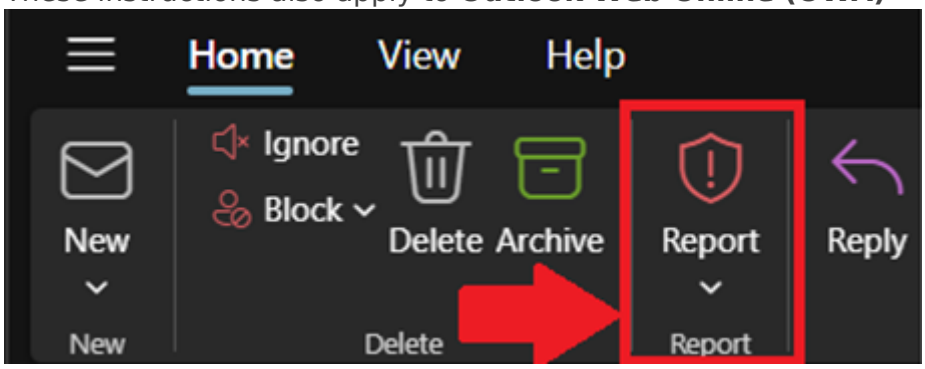
Outlook (Classic)

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)**



Security Awareness

PIEDMONT UNIVERSITY
SECURITY AWARENESS GUIDE

Be a Lion. Not a Number

WELCOME!
STOP. THINK. VERIFY.
Don't act on urgent or unexpected messages without confirmation!

1 PASSWORD SAFETY
One password can open many doors.

- Do not write passwords on sticky notes.
- Never share passwords with others.
- Use strong, unique passwords.
- Enable MFA when available.
- Lock your computer when away.

A STICKY NOTE IS NOT A PASSWORD MANAGER.

2 EMAIL & PHISHING
Think before you click.

- Be cautious with unexpected links.
- Verify unusual requests.
- Do not open suspicious attachments.
- Watch for fake login pages.
- Report suspicious emails to IT.

URGENCY IS A COMMON TACTIC.

3 PHYSICAL SECURITY
Security exists in physical spaces too.

- Do not hold secure doors open.
- Wear your university ID visibly.
- Report broken badge readers.
- Secure offices and classrooms.
- Do not leave devices unattended.

FAMILIAR FACES ARE NOT VERIFICATION.

4 SHARED DEVICE & DESK SAFETY
Protect student and university information.

- Log out of shared computers.
- Remove printed documents promptly.
- Keep sensitive paperwork secure.
- Avoid leaving devices unlocked.
- Keep student information private.

LOCK BEFORE YOU WALK.

5 AI & DEEPFAKES
AI can imitate someone you trust.
Independent verification is the lock it cannot pick.

- Trust the request only after you verify it another way.
- AI can fake a voice, face, email, or video.
- Before sending money, sharing information, or taking urgent action, contact the person or organization through a trusted channel you already know.

VERIFY ANOTHER WAY. PROTECT YOURSELF.

IF SOMETHING FEELS OFF:

STOP
Pause and look for signs of suspicious activity or requests.

VERIFY
Verify the request using a trusted contact or source.

REPORT
Report it to IT right away. You may prevent harm to others.

STAY CONNECTED. STAY INFORMED.
Bookmark these resources and check back often!
We're here to support your success!

IT HELP DESK
ITSupport@piedmont.edu
706-894-4205
ITSupport.piedmont.edu