TASK 2: Analyze a Phishing Email Sample

**Objective:** Identify phishing characteristics in a suspicious email sample.

**Tools:** Free online resources.

**Prepared by:** P. SUSMITHA,

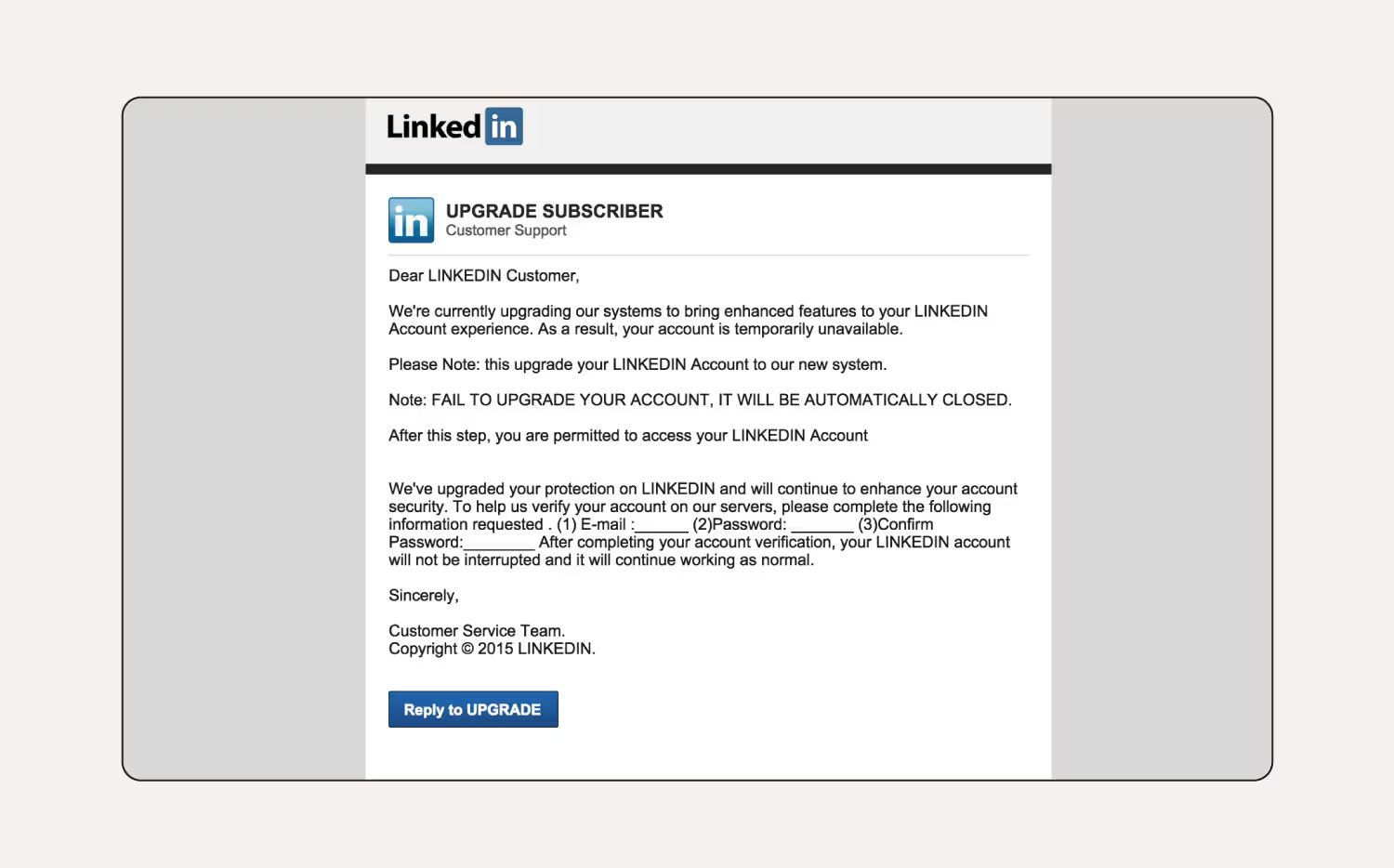
**Date:** 22/10/2025.

**About Phishing**

* **PHISHING:** Phishing is a cybercrime where an attacker uses deception, primarily through email, text, or phone calls, to trick individuals into giving up sensitive information.
* **Types of Phishing:**
* **Email Phishing (Deceptive Phishing):** Large, random number of users.
* **Spear Phishing:** A specific individual or small group.
* **Vishing:** Targets via Voice (phone calls).
* **Smishing:** Targets via SMS (text messages).
* **Spear Phishing:** To a specific user targeting.
* **Tailgating/Piggy backing:** When unauthorized person gains physical access to restricted area by following authorized person.
* **Baiting:** Tempting to trick victims.

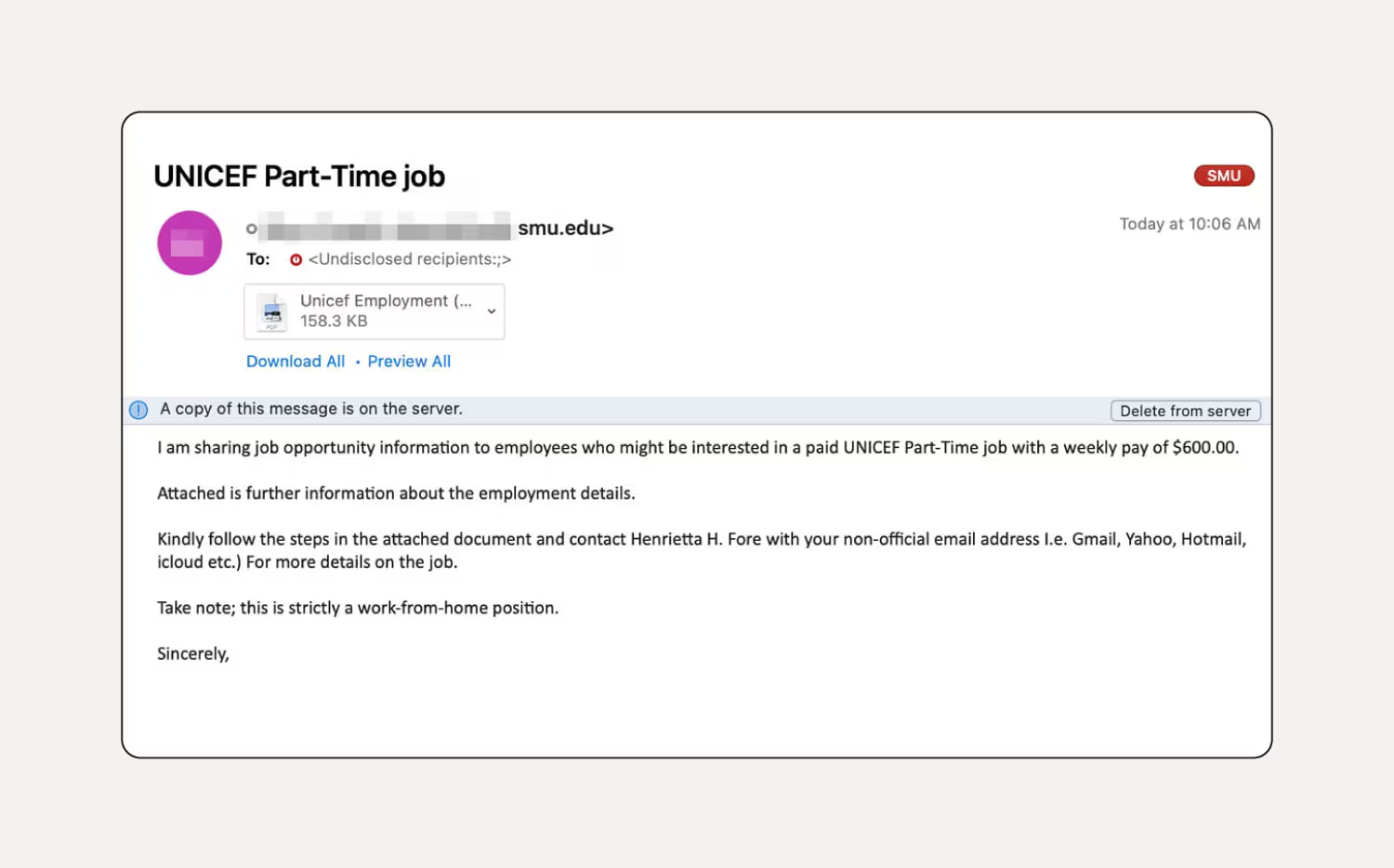
**Examples:**

**1.Social media phishing emails**

****

* Social media phishing emails can be the launchpad for Facebook, LinkedIn, Instagram scams.
* **Identification of Phishing Email:**
* The user’s name isn’t specified in the greeting.
* The business name is in capital letters throughout the email.
* Awkward Phrasing: In Email, “temporarily unavailable” shows suspicious activities.
* Grammatical issues: “upgrade your LINKEDIN Account **to**  our new system”, here word “to” is missing, leading to an incomplete thought.

**2. Fake job scams:**

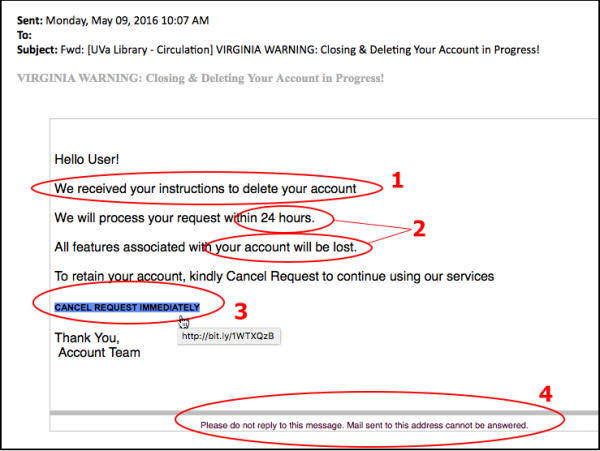
****

* Fake job phishing emails, often promising high pay and no skills required, aim to lure people into work-from-home scams.
* They also include attachments with malware.
* **Identification of Phishing Email:**
* This email sent from a suspicious email address, it should come from a .org instead of a .edu address.
* The attachment is titled “Unicef Employment,” which doesn’t match the organisation’s branding.
* Awkward Phrasing: The phrasing "sharing job opportunity information to employees" is slightly awkward.
* Grammatical issues: The list of email providers is closed with a parenthesis ) but has no opening parenthesis. "etc.)" is followed immediately by a capitalized "For," indicating a run-on sentence.

## **3. PayPal phishing emails:**The user’s name hasn’t been specified and it’s a generic greeting. The first sentence provokes a sense of urgency, hoping the user acts without thinking.

* **Identification of Phishing Email:**
* **Awkward Phrasing:** “You have to confirm” sounds demanding and less professional than a standard directive.
* The list of activities is clunky and unprofessional.

**4. Example** **Spam/Phishing Email Message:**



* **Identification of Phishing Email:**
* The tone of urgency, indicated by a 24-hour deadline, along with an implied threat, indicated by the words "your account will be lost".
* A tone of urgency, veiled threat to those who do not act will generate fear, a key tactic phishers use to deceive us, and to push us to act without thinking.

## **How to recognise a phishing email:**

* **Incorrect Email Address:** An unfamiliar, mismatched, or misspelled email address/domain (e.g., micros0ft.com).
* **Urgency & Threats:** Language demanding immediate action or threatening negative consequences (e.g., "Account suspended in 2 hours!").
* **Links:** A visible hyperlink text that does not match the actual destination URL when you hover over it (the most critical sign).
* **Attachments:** Unexpected files, especially with suspicious extensions like .zip, .exe, or .js.
* **Errors:** 3.Obvious spelling mistakes, poor grammar, or unprofessional formatting.
* **Personal Info Request:** Requests for sensitive data like your password, PIN, or credit card number directly via email, which legitimate companies won't ask for.

### 

### 

### 

### 

### **What do I do if I clicked a suspicious link in a phishing email?**

* **Change your password:** [Create a secure password](https://uk.norton.com/blog/how-to/how-to-choose-a-secure-password) using a combination of numbers, letters, and symbols to help preventing the credential stuffing.
* **Run antivirus software:** A thorough scan will help detect different [types of malware](https://uk.norton.com/blog/malware/types-of-malware) that may have infected your device.
* **Enable two-factor authentication (2FA):** This will add an extra layer of protection against hackers trying to crack your account.
* **Report the phishing email:** Report suspicious emails to the National Cyber Security Centre (NCSC) by forwarding them to [report@phishing.gov.uk](mailto:report@phishing.gov.uk).

-------\*\*\*\*------