# Task 2

Phishing Email Sample

**From:** NetfIix Support [support-team@ntflx-secure.com](mailto:support-team@ntflx-secure.com)

**Subject:** Urgent: Your Acount is on Hold!

**Body:**

Dear Valued Customer,

We have detected unusal activity on your NetfIix account. For you're protection, we have temporarily suspended your account.

To restore access, you must verify you're payment details immediately. Please click the link below to update your information.

https://ntflx-secure.com/login-update

Failure to do so within 24 hours will result in permanent account termination.

Sincerely, The NetfIix Security Team

Analyzing the Sample Email

* **Sender's Email Address:**
  + The sender's email is support-team@ntflx-secure.com. While it looks plausible, official Netflix emails typically come from @netflix.com. The domain ntflx-secure.com is a **spoofed domain** designed to trick you.
* **Urgent or Threatening Language:**
  + The email uses phrases like **"Urgent," "temporarily suspended,"** and threatens **"permanent account termination"** if you don't act within 24 hours. This creates a sense of panic, a common social engineering tactic.
* **Spelling and Grammar Errors:**
  + There are several mistakes:
    - "unusal" should be "unusual."
    - "you're protection" should be "your protection."
    - "verify you're payment details" should be "verify your payment details."
    - "NetfIix" uses a capital "i" instead of an "l".
* **Suspicious Links:**
  + The link hxxp://ntflx-secure.com/login-update is suspicious. Legitimate Netflix links would lead to netflix.com. Attackers register similar-looking domains to host fake login pages. Hovering over the link would reveal this potentially malicious URL.
* **Generic Greeting:** 
  + The email starts with "Dear Valued Customer." A real company like Netflix would likely address you by your name.