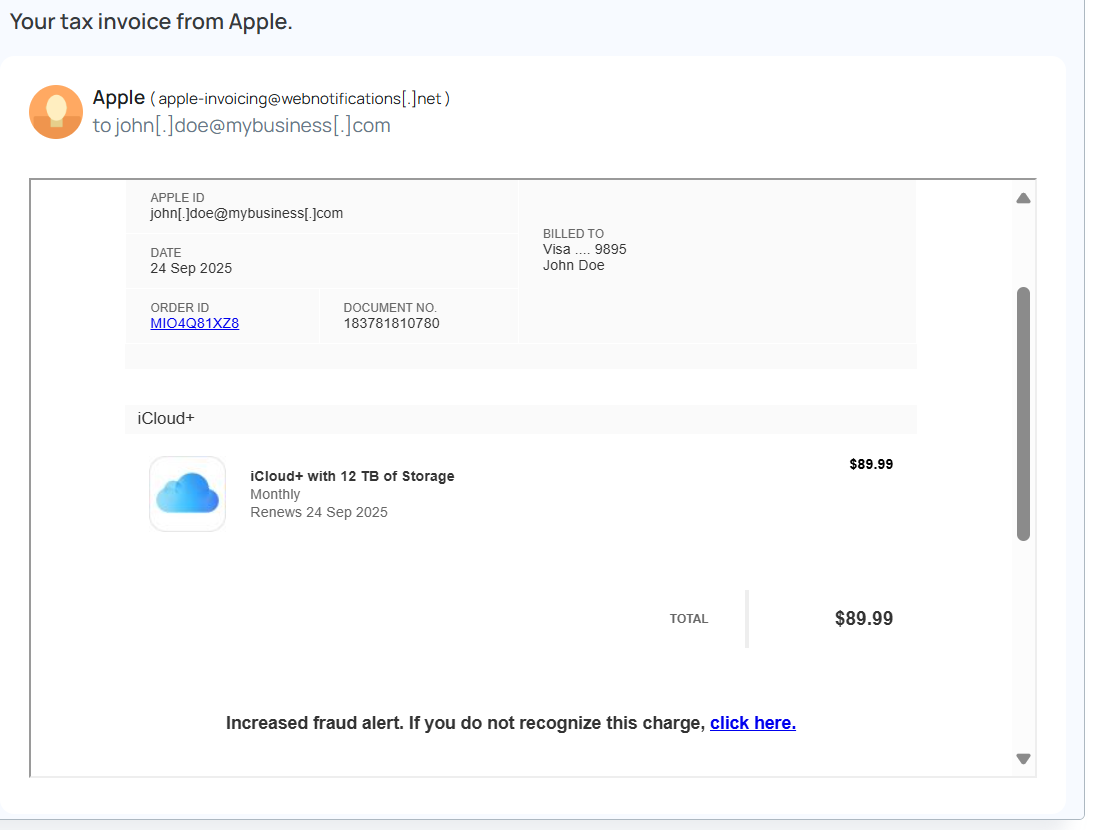
Cyber Security Internship Task-2

Objective: Identify phishing characteristics in a suspicious email sample.



1. Sample phishing email

Above mail

1. Sender’s email address

The email is from **apple-invoicing@webnotifications.net**. That’s **not Apple’s real domain** (which would be something like @apple.com). This is a big sign it’s fake.

1. Email headers

From the mail we can’t see the full headers, but if you checked them in Gmail/Outlook you’d likely see things like:

* “From” doesn’t match the “Return-Path.”
* SPF/DKIM checks fail.  
  That’s another red flag.

1. Suspicious links/attachments

There are no attachments here, but there are links:

* The **ORDER ID** link.
* The “**click here**” under the fraud alert.

Phishing emails often hide a malicious site behind these links.

1. Urgent or threatening language

The line “**Increased fraud alert. If you do not recognize this charge, click here.**” is classic scare-tactic language to pressure you into clicking.

1. Mismatched URLs

If you hover over the links (without clicking), you’ll almost certainly see that they don’t go to apple.com but some strange domain instead. That mismatch is a giveaway.

1. Spelling/grammar errors.

This one doesn’t have obvious spelling mistakes, but phishing emails don’t always — some are written very cleanly now.

1. Summary of phishing traits

 Fake sender domain (webnotifications.net instead of apple.com).

 Urgent warning to trick you into acting fast.

 Links that don’t match Apple’s real website.

 Invoice details (12 TB iCloud for $89.99) that don’t match Apple’s real pricing.

 It looks like an Apple invoice but lacks Apple’s real email security signs.