Introduction:
As part of my cybersecurity internship, I analyzed a phishing email sample to understand how attackers trick users and how we can detect and prevent such threats. This report summarizes my observations and insights from the analysis.

Email Description:
I found a phishing email that pretended to be from a popular online service, claiming I had won a reward and asking me to click on a link to claim it.

Indicators of Phishing:
Spoofed Email Address:

The sender’s name looked genuine, but the actual email address was suspicious (e.g., support@reward-claim-now.xyz), which didn’t match the real domain of the company.

Email Header Discrepancies:

I used an online email header analyzer to check the source. The "Return-Path" and "Received" fields didn’t match the official servers of the claimed company.

Suspicious Links:

The email contained a link that appeared legitimate at first glance. However, when I hovered over it, I saw it redirected to an unknown, shady-looking domain.

Urgent Language:

The email used phrases like “URGENT: Your reward expires in 24 hours” and “Click now or lose your prize,” clearly trying to trigger a fear-of-missing-out response.

Mismatched URLs:

The text said one thing, but the actual link went somewhere else. This is a classic phishing trick.

Grammar and Spelling Errors:

There were several mistakes in the email, such as “Congratulation” instead of “Congratulations,” and weird punctuation.

Unusual Attachments:

Though this email didn’t include an attachment, many phishing emails do. I learned that these often contain malware or ransomware.

What I Learned:

This exercise helped me understand the signs of phishing emails and how social engineering is used to manipulate users. It made me more aware of how attackers try to exploit human behavior and technical loopholes.

Key Takeaways:
Always hover over links before clicking.

Check the sender’s domain carefully.

Look out for urgency, fear tactics, and bad grammar.

Use tools like header analyzers to dig deeper.

Tools I Used:
Google header analyzer: https://mxtoolbox.com/EmailHeaders.aspx

Sample phishing email (from open source phishing archives)