**Task 2: Analyze a Phishing Email Sample.**

1.Obtain a sample phishing email (many free samples online).

2.Examine sender's email address for spoofing.

3.Check email headers for discrepancies (using online header analyzer).

4.Identify suspicious links or attachments.

5.Look for urgent or threatening language in the email body.

6.Note any mismatched URLs (hover to see real link).

7.Verify presence of spelling or grammar errors.

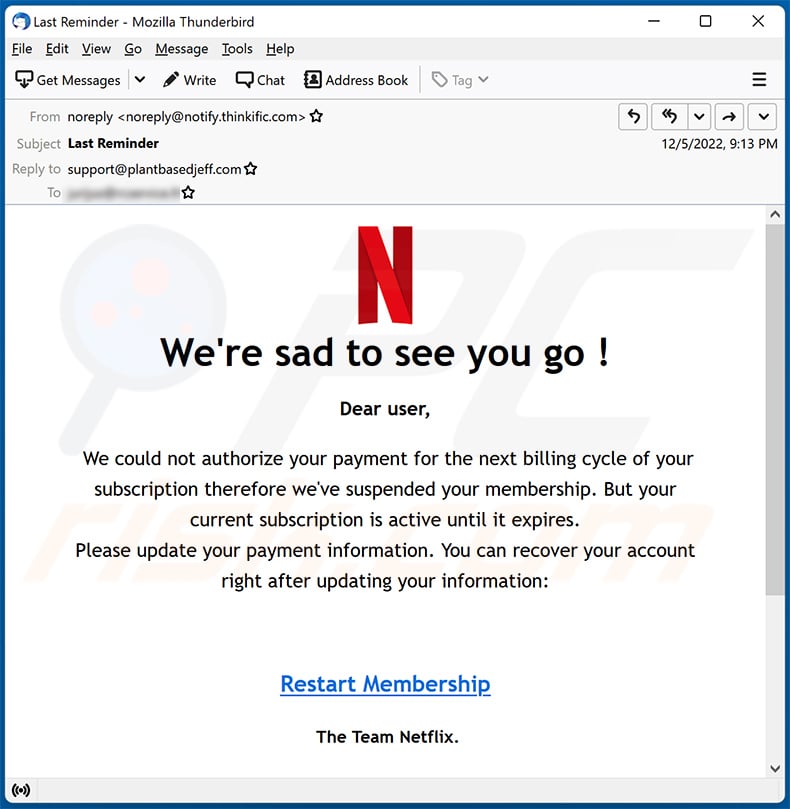
8.Summarize phishing traits found in the email.

**Suspended account phishing emails**

A suspended account phishing email scam is a cyber attack where scammers pose as legitimate companies claiming your account is suspended. They commonly cite reasons like suspicious activity, expired payment methods, or terms of service violations.

Once you click a link, you’ll be redirected to a fake website that looks like a legitimate login page, where scammers capture sensitive information.

1. **A phishing email about a suspended Netflix account.**

****

**2.Examine sender's email address for spoofing.**

Actual From: [noreply@notify.thinkific.com](mailto:noreply@notify.thinkific.com)

**Not a Netflix domain.**

Thinkific is an online course platform and not related to Netflix.

**Clear sign of email spoofing or abuse of a third-party mailer.**

**3.Check email headers for discrepancies (using online header analyzer).**

You need full headers for a complete check, but here's what is suspicious:

**Mismatch between display name ("Netflix") and actual sender (notify.thinkific.com).**

Reply-to is support@plantbasedjeff.com—completely unrelated to Netflix.

This is often used to redirect user replies or collect stolen credentials.

**4.Identify suspicious links or attachments.**

Anchor text: "Restart Membership"

Hovering would likely reveal a non-Netflix URL, possibly leading to a fake login/payment page.

No visible link, but phishing emails often hide links with legitimate-looking text.

**5.Look for urgent or threatening language in the email body.**

"We're sad to see you go!" → emotional manipulation.

We could not authorize your payment" → financial pressure.

**"Recover your account right after..." → sense of urgency.**

Classic urgency tactic to make the user act quickly without thinking.

**6.Note any mismatched URLs (hover to see real link).**

**Display text is clean (e.g., "Restart Membership"), but phishing emails typically redirect to fake domains.**

**Hovering on real emails should show netflix.com, not an unknown or shortened URL.**

**7.Verify presence of spelling or grammar errors.**

**Minor issue:** “The Team Netflix.” (should be “The Netflix Team”).

Sentence flow is awkward in some places.

**Subtle grammar issues are often a red flag for phishing scams.**