🛡️ Phishing Email Analysis Report
Cyber Security Internship – Task 2
Sample Email: Netflix Password Expiration (Simulated via CanIPhish)

---

1. 📧 Sender's Email:
- **Appears as**: `netflix@webnotifications.net`
- **Issue**: Not an official Netflix domain. This is a lookalike/suspicious domain.

---

2. 📝 Email Subject:
- **Subject**: "Netflix Password Expiring in 3 Days"
- **Analysis**: Creates unnecessary urgency to trick the user into acting quickly.

---

3. 📄 Email Body:
- The email claims your Netflix password is about to expire.
- It asks the user to click a link to reset the password.
- **Red Flags**:
- Fake urgency
- Spoofed branding (Netflix logo)
- Pressure to act quickly

---

4. 🔗 Suspicious Links:
- **Displayed Link**: `https://netflix.com/reset-password`
- **Real Link (on hover)**: `https://netflix-password-reset[.]info/login`
- **Analysis**: The link does not belong to the real Netflix domain. It’s a phishing URL.

---

5. 🧠 Language & Tone:
- Language is **urgent and threatening**.
- Example: “You will lose access to your account if you do not reset now.”
- Designed to trigger emotional reaction and cloud judgment.

---

6. □ Social Engineering Indicators:
- **Emotional Triggers**: Urgency and fear
- **Fake Authority**: Pretends to be Netflix support
- **Personalization**: Uses recipient’s name to appear real

---

7. □ Spelling/Grammar:
- Minor issues, like:
- "Your account will be terminate" □ should be "terminated"

---

8. □ Screenshots:
- Email interface showing:
- Sender and subject
- Hovered link
- Fake reset button

(Upload your screenshots as separate files in the repo)

□ Conclusion:
This is a **phishing email** designed to steal user credentials by:
- Spoofing Netflix branding
- Using an urgent tone
- Embedding a malicious link

Phishing Traits Found:
- Spoofed email domain
- Urgency in language
- Mismatched links
- Social engineering tactics
- Grammar errors

Tools Used:
- [CanIPhish Simulator](https://caniphish.com)
- Manual inspection (hover link, email structure)