Task 2 Title:

Phishing Awareness Training Module

Task Requirement:

As part of the CodeAlpha Cybersecurity Internship, Task 2 required us to:

1. **Create a Presentation or Online Module** focused on phishing awareness
2. **Explain how to recognize phishing emails and fake websites**
3. **Educate users about social engineering tactics** used by attackers (e.g., urgency, fear, impersonation)
4. **Include real-world examples** of phishing attacks for context
5. **Design interactive quizzes** to test understanding and engage users
6. **Use screenshots and visuals** where possible to compare real vs. fake content

---

Objective:

To create an engaging, educational module that helps users identify and defend against phishing attacks.

What I Did:

Developed a Slide-Based Presentation:

- Explained what phishing is and how it works
- Broke down the anatomy of a phishing email
- Showed how fake websites trick users
- Educated on social engineering tactics (urgency, fear, curiosity)
- Shared real-world examples of phishing attempts:
    - **Example 1:** Fake PayPal email with misspelled URL
    - **Example 2:** Fake bank login page asking for sensitive info
    - **Example 3:** CEO fraud email requesting urgent wire transfers
- Included screenshots of fake vs real messages

Created an Interactive Google Forms Quiz:

- Reinforced key lessons using 4 multiple-choice questions
- Link to quiz: https://forms.gle/Qf93KxaYf6Fu4ugr7

Presented with Google Slides:

- Slide Deck Link: https://docs.google.com/presentation/d/1Bys8cgknez7jEPWxwfN9PWJcqWh5HN7ajz_APhDVVSc/edit?usp=sharing

---

What I Learned:

- How phishing attacks manipulate human psychology
- Techniques used in social engineering (authority, urgency, trust)
- How to critically examine URLs, headers, and email formatting
- The value of user education in cybersecurity awareness
