Practical Cybersecurity: Team-Based Activity

Activity Name: Build A Secure Network

Objective: Work as a team to design a secure network for a company while considering real-world cybersecurity threats.

Team Members –

1.
2.
3.
4.
5.

Scenario:

You are the cybersecurity team for Hogwarts Inc., a growing company handling customer transactions in the wizarding world, storing private employee records, and allowing remote work. Recently, minions of the Dark Lord have attempted phishing attacks and tried to steal sensitive data from your company. Your mission is to design a network security plan to:

- Protect sensitive data (Ex – Customer Identification, Transactions and Banking Information)
- Ensure secure communication between the company and customers, and between the company employees
- Block hackers from accessing the system

Part 1: Network Design

- Use the space below to explain what protective measures you include in a basic network setup for the company.

- Include at least 3 key security measures and briefly explain their purpose and functionality on how they protect the company from cyber threats.

Key Security Elements to Consider:

- Firewalls – Where will you place them in your network?
- Encryption – What data should be encrypted? Why?
- Authentication – How will employees log in securely?
- Public Wi-Fi Policy – How can remote employees stay safe?
- Incident Response Plan – What should the company do if a cyberattack happens?

Part 2: Cybersecurity Challenge

At halfway point, your team will receive a cybersecurity incident scenario and must adjust your security plan accordingly.

Your Assigned Cybersecurity Incident:

(Your will be assigned one of the following)

1. A phishing email successfully stole an employee's password.

   How will your team respond?

2. Hackers gained access to an unencrypted database.

   What security measures should change?

3. An employee connects to company systems using public Wi-Fi.

   What risks does this pose, and how will you mitigate them?

Answer below:

Part 3: Final Reflection Questions (Bonus 1% to overall course grade if all 3 are answered):

What was the biggest security risk your team identified?

Did any team forget to secure a critical area?

If you had unlimited resources, what additional security measures would you implement?