Malware Prevention and Response Guide

Section 1: What is Malware?

Define malware and explain the different types (e.g., viruses, ransomware, spyware, trojans).

Provide real-world examples from the simulation or famous malware attacks (e.g., WannaCry, NotPetya).

Section 2: How Does Malware Spread?

Describe how malware infects systems (e.g., phishing emails, malicious websites, infected USB drives).

Discuss the role of social engineering in spreading malware, referencing the tactics seen in the simulation.

Section 3: Malware Prevention Techniques

Outline key prevention techniques such as:

- Antivirus software
- Regular updates
- Safe browsing habits
- Employee training

Rank these strategies in order of importance and justify your ranking.

1. _____
2. _____
3. _____
4. _____

Why did you rank these this way?

_____

_____

_____

Section 4: Responding to a Malware Attack

Step-by-step guide on how to respond to a malware infection:

- Isolate infected systems.
- Run antivirus scans.
- Use backups.
- Contact professionals.

Create a checklist based on your experience from the simulation.

Checklist:

- _____
- _____
- _____
- _____

Section 5: Case Study

Choose a real-world malware attack (such as WannaCry or Stuxnet) and explain:

- How the attack spread.
- What damage it caused.
- How it was contained.
- What prevention strategies could have stopped it before causing damage.

_____

_____

_____

_____

Reflection Questions:

1. What prevention strategies do you think are most effective in preventing malware infections?

2. What was the most surprising thing you learned about malware from your case study?

3. How would you apply the lessons learned in real-life situations to protect systems from malware?

Checklist for Responding to a Malware Attack

1. Isolate infected systems.
2. Run antivirus scans.
3. Disconnect from the network if necessary.
4. Restore from backups (if available).
5. Monitor systems for further suspicious activity.
6. Contact cybersecurity professionals.