VIRUS AND MALWARE PROTECTION CURRICULUM

Week 1: Introduction to Cybersecurity Threats

- Objective: Understand the landscape of cybersecurity threats, with a focus on viruses and malware.
- Introduction to common types of malware: viruses, worms, Trojans, ransomware, and spyware.

Week 2: Fundamentals of Cybersecurity

- Objective: Explore the basic framework for understanding safeguards
- Overview of the 6 fundamental concepts:
    1. Confidentiality
    2. Integrity
    3. Availability
    4. Physical Safeguards
    5. Technical Safeguards
    6. Administrative Safeguards

Week 3: Securing Endpoints and Networks

- Objective: Understand how to extend protection beyond individual devices.
- Introduction to endpoint security: firewalls, intrusion detection/prevention systems.
- Network-level protection strategies.

Week 4: Guest Speaker – Sandia Labs

Week 5: Technical Safeguard: Anti-malware software

- Objective: Delve into advanced techniques employed by anti-malware tools for proactive defense.

Week 6: Student Presentations

- Students will make a presentation on what they've learned.

By the end of this 6-week curriculum, participants will have not only gained a comprehensive understanding of virus and malware protection but also practical skills in configuring antivirus software, implementing advanced protection techniques, securing networks, and responding to and recovering from malware incidents.