Physical Security Module

Module Learning Outcomes:

- #3: Explain different types of attacks on computing systems.
- #5: Realize the importance of password and username management and apply effective approaches to increase their security.
- #11: Develop skills needed to defeat various mal- and social engineering attacks.
- #12: Apply the knowledge gained in solving real-world, scenario-based problems.
- #13: Realize the important role humans play in the digital world and understand how to minimize accidental and intentional human errors.

The Module addresses the following First Principles:

- #4: Least Privilege
- #5: Layering
- #7: Information Hiding

Description:

This module on physical security will allow students the opportunity to develop an upgrade to the physical security system of an office building. These upgrades will included changes to policy,

Be able to develop a sound security policy that addresses the overall physical threat to an organization's computer resources.

Learner-Centered Classroom:

In this module students will work in teams to test and design an upgrade to an existing physical security system. Students will be challenged to upgrade a facility to increase its security posture. As part of this team building exercise, students will test their upgrade using computer modeling software. A major component of this module will be the introduction of the design and evaluation process as developed by the Department of Energy. Students will be instructed on how to apply this process for their own protection and also the protection of personal assets such as a laptop or computer system. Students will be introduced to the three types of adversaries: outsiders, insiders, and outsiders in collusion with insiders, and the unique challenges each brings. a 6(u)133. n r i e