SEMtech!

Student Engagement & Mentoring in Technology

Activity 1: "Secure or Sabotage?" (Scenario-Based Security Audit)

Objective: Identify and evaluate secure vs. insecure device practices.

How it works:

- Prepare a series of **realistic device usage scenarios** (e.g., "Jamie uses the same password for all apps" or "Morgan updates antivirus definitions weekly").
- Students work in pairs or small groups to **classify each behavior** as:
  - **Secure Practice**
  - **Needs Improvement**
- For each item, they must explain:
  - What's secure or insecure?
  - Which principle does it relate to (passwords, antivirus, firewall, updates)?
  - What corrective action should be taken?

Extension: Create a "Top 5 Secure Habits" list based on group discussion.

STEM Linkage: Supports behavioral cybersecurity and risk analysis—key skills for cybersecurity analysts and IT support professionals.

Activity 2: "Cyber Hygiene Checklist Relay"

Objective: Reinforce device security best practices through movement and collaboration.

How it works:

- Post different **security categories** at stations around the room:
  1. **Passwords & MFA**
  2. **Antivirus & Firewalls**
  3. **Software & Updates**
  4. **Web Browsing & Software Sources**
  5. **Physical Security & Tracking**
- Each team rotates through the stations, adding:
  - One **best practice** under each category
  - One **real-world example** (e.g., "Using Face ID to unlock a phone" under Passwords)
- At the end, review the complete checklist and identify top critical habits.

SEMtech!
Student Engagement & Mentoring in Technology

STEM Linkage: Engages kinesthetic learners and models procedural cybersecurity thinking—vital for systems administrators and tech educators.

Activity 3: "Patch the Gaps!" (Interactive Threat Simulation)

Objective: Simulate identifying and remediating vulnerabilities in mobile devices or workstations.

How it works:

- Students are given a **mock audit report** describing a vulnerable device (e.g., "Outdated OS, default password still enabled, no antivirus installed").
- In teams, they must:
    1. Identify all vulnerabilities
    2. Recommend remediation steps
    3. Prioritize actions (Which should be fixed first? Why?)
- Include terminology like **data at rest**, **remote wipe**, and **safe web browsing** in the challenge.

Debrief: Discuss how these security gaps could lead to real incidents (e.g., stolen data, malware infections).

STEM Linkage: Builds analytical and remediation skills critical for roles in IT security, support, and network administration.

Bonus Integration:

Tie these activities into a **cybersecurity capstone project**, where students create a personal or organizational **Device Security Policy**, incorporating:

- Password policies
- Update and patching schedules
- Mobile device management (MDM) guidelines
- Acceptable use rules for safe browsing