Lesson Plan: Cyber Security Threats

Teacher: Marcello Goccia
Grade Level: Grade 10 Students of IGCSE Computer Science
Number of Students: 8
Lesson Duration: 80 minutes

---

1. Lesson Overview

This lesson introduces students to a range of cyber security threats, including brute-force attacks, data interception, hacking, and DDoS attacks. Through a combination of real-world scenarios, group research, and collaborative problem-solving, students will explore the processes and aims of these threats.

---

2. Desired Learning Outcomes

By the end of this lesson, students will be able to:

- Identify and describe a range of cyber security threats (e.g., brute-force attacks, hacking, DDoS attacks).
- Explain the processes and aims of these threats.
- Analyse real-world examples of cyber security incidents.
- Collaborate to propose strategies to mitigate these threats.

---

3. Teaching and Learning Strategies

This lesson follows the **5E Model (Engage - Explore - Explain - Elaborate - Evaluate)** framework.

1) Engage (10 minutes) – Capturing Interest

Objective: Hook students with real-world cyberattack examples.

- **Starter Activity: Cyber Attack News Flash**
  - Show a **real-world hacking incident** (example in this link).
  - Discuss: *"What do you think happened? How was the system compromised?"*
- **Quick Discussion:** Ask students:
  - *"Have you ever received a suspicious email or message? Why do cybercriminals attack systems?"*

2) Explore (20 minutes) – Hands-on Investigation

Objective: Allow students to explore cybersecurity threats through research and analysis.

- **Cybersecurity Threats Exploration Task:**
  - Students work in **small groups**, each assigned a **specific cybersecurity threat**:
    Brute-force attack, Data interception, DDoS attack, Hacking
- **Group Research & Discussion:**
  - Each group researches their assigned threat and prepares a short summary (3-4 minutes each) explaining: How the attack works, examples of real-world cases, consequences & prevention methods

3) Explain (15 minutes)

Objective: Provide a clear understanding of **cyber threats and defences**.

- **Teacher-Led Explanation**
    - Summarize each **cybersecurity threat**, reinforcing student research.
    - Use **real-world examples** (e.g., when brute force is used, or major DDoS attacks).
    - Invite students ask questions and clarify doubts.
- **Visual Demonstrations:**
    - Display a **brute-force password cracking simulation** to illustrate the **importance of strong passwords**.

4) Elaborate (25 minutes) – Application & Problem-Solving

Objective: Apply cybersecurity knowledge to real-world problem-solving.

Activity: Cybersecurity Defence Consultant

- **Scenario:** A company has suffered a cyberattack! Each student group acts as **cybersecurity consultants**.
- **Task:**
    - **Analyse the attack:** Identify which threat occurred.
    - **Explain the impact:** What damage was caused?
    - **Propose a defence plan:** Suggest how the company should improve its security.

5) Evaluate (10 minutes) – Assessing Understanding

Objective: Measure student learning through discussion and reflection.

Quick Cybersecurity Quiz

- Multiple-choice and short-answer questions on cyber threats and prevention.

Exit Ticket Reflection

- **Prompt:** "Which cybersecurity threat do you think is the most dangerous today, and why?"
- Students submit a **1-minute written response**.

---

4. Resources & Materials

- Presentation Slides (for theoretical concepts and explanations)
- Videos or webpages explaining cyber security threats.
- Handouts with key terms and definitions.
- Access to computers or tablets for research.
- Group activity worksheets.

---

5. Vocabulary & Cross-Curricular Links

- **New Vocabulary:** Cybersecurity, Brute-force attack, Malware, DDoS Attack,, Hacking, Perpetrator, Biometric Password, Biometric Device, Two-step Verification, Botnet, Packet Sniffer.
- **Cross-Curricular Connections:**

    Business Studies: Cybersecurity in financial transactions

    - **Ethics**: The moral implications of hacking

6. School-Wide Learning Outcomes

- **Critical Thinking**: Analysing cybersecurity threats and evaluating countermeasures.
- **Digital Citizenship**: Understanding ethical cybersecurity practices.
- **Collaboration**: Working in teams to assess security scenarios and problem-solve.