

# 1. Konfydence: The HACK Lesson Plan

(Teacher-Facing Core Document)

## Target Audience

Students ages: 12–18

**Duration:** 45 minutes (one standard class period)

## Learning Objective

To help students move from *knowing* digital safety rules to *practicing* recognition of psychological manipulation patterns — building the habit of pausing before reacting under pressure.

This lesson focuses on **recognition and response**, not technical cybersecurity skills. It complements existing digital citizenship and online safety curricula.

---

## Lesson Structure

### 1. Introduction: The Intelligence Myth (5 minutes)

#### The Hook

Ask students:

“Who here thinks they’re too smart to be scammed?”

#### The Reality Check

Explain that scams don’t target lack of intelligence.

They target:

- Busy people
- Helpful people
- People responding to authority or urgency

#### Key Message

Scammers don’t just hack computers.

They **HACK people** — by triggering emotional shortcuts.

## 2. Teaching the HACK Framework (10 minutes)

Introduce the four psychological triggers scammers use to override rational thinking:

### **H — Hurry**

Artificial urgency that pressures fast action

Examples: “Act now,” “Final notice,” “2 minutes left”

### **A — Authority**

Use of titles or roles to stop questioning

Examples: “School admin,” “IT support,” “Police”

### **C — Comfort**

Familiar names, logos, or friendly tone that lowers guard

Examples: “Friend,” “Teacher,” “Trusted brand”

### **K — Kill-Switch Emotions**

Fear, excitement, or shame that shuts down logic

These are **HACK signals**, not proof of wrongdoing.

The goal is noticing them — not being perfect.

---

## 3. Interactive Gameplay: Security Skill Kit (20 minutes)

### **Activity Setup**

Students work in small groups using Konfydence Security Skill Kit (SSK) scenario cards.

### **For Each Scenario, Students:**

1. Read the scenario aloud
2. Identify which HACK signals are present
3. Choose the *safer* vs. *riskier* response

### **Guided Discussion Prompts**

- “Which HACK signal stood out first?”
- “What made this feel believable?”
- “Where did the pressure come from?”

Teachers circulate and encourage reflection, not judgment.

*Note for Teachers:* If a student reveals they have been a victim of a real scam during the discussion, thank them for their confidence and follow the school's standard reporting protocol. Remind the class that reporting is the ultimate "Kill-switch" bypass.

#### **4. Reflection: The Permission to Pause (10 minutes)**

##### **Core Skill**

Students learn that confidence is not reacting fast — confidence is **pausing under pressure**.

##### **Key Rule**

“If you feel a HACK signal, pause first.”

##### **Closing Message**

Mistakes are part of learning.

Speaking up, asking questions, and verifying information are signs of confidence — not failure.