1. Simulated Web Browser Sandbox

Objective: Teach browser configuration and security settings through guided simulation.

How It Works:

- A simulated browser interface (HTML/JS-based) allows students to:
    - Set a homepage
    - Change the default search engine
    - Enable/disable extensions
    - Manage cookie and pop-up settings
    - Enter a URL and navigate to simulated content
- Prompts guide students to tasks like:
  "Enable Do Not Track and configure your browser to block all third-party cookies."

Why It Works:
Provides **hands-on practice** with browser settings in a safe, sandboxed environment—ideal for developing **practical configuration skills** tested on the exam.

---

2. Safe or Suspicious? Drag-and-Drop Security Challenge

Objective: Help learners identify safe browsing practices and security warnings.

How It Works:

- Students drag and drop browser messages or URLs into **"Safe"** or **"Suspicious"** categories.
- Examples:
    - `"https://mybank.com"` Safe
    - `"http://login-paypaI.com"` Suspicious
    - `"Certificate not valid"` warning Suspicious
    - `"Do Not Track enabled"` Safe
- Immediate feedback with explanations reinforces correct decisions.

Why It Works:
Sharpens awareness of **phishing threats**, **HTTPS importance**, and **certificate warnings**, which are key for cybersecurity literacy and tested in ITF+.

3. Browser Settings Scenario Quiz

Objective: Apply browser knowledge in real-world scenarios.

How It Works:

- Students are presented with **scenario-based questions**, such as:

  "Sam notices that every time she opens her browser, it loads an unfamiliar homepage. What setting should she change?"

  o A) Extensions
  o B) Homepage
  o C) Search Engine
  o D) Downloads
  o **Correct: B**
- Questions cycle through topics like downloads, history, incognito mode, and appearance settings.

Why It Works:
Combining **reading comprehension** with **applied knowledge**, helping students make informed decisions under test conditions and in real-life use.

Summary Table

Activity Name	Focus Area	Interaction Type
Simulated Web Browser Sandbox	Configuration and setup	Guided simulation
Safe or Suspicious? Drag-and-Drop	Security and safe browsing practices	Interactive classification
Browser Settings Scenario Quiz	Troubleshooting and user scenarios	Scenario-based quiz