**Activity 1: Icebreaker Quiz - Cybersecurity Awareness**

**Objective:** Engage participants and assess their baseline cybersecurity knowledge.  
**Time:** 10–15 minutes  
**Materials:**

* Quiz platform (e.g., Kahoot, Google Forms, or printed quiz sheets)
* Projector or screen (if done as a group activity)

**Instructions:**

1. **Preparation:**
   * Create a quiz with 8–10 questions covering basic cybersecurity topics. Example questions:
     + *What is phishing?*
     + *What is a strong password?*
     + *True or False: Public Wi-Fi is always secure.*
   * Include a mix of multiple-choice, true/false, and scenario-based questions.
2. **Execution:**
   * If using a platform like Kahoot, share the access code with participants.
   * Conduct the quiz as a group or individually.
   * For printed quizzes, distribute sheets and set a 10-minute timer.
3. **Discussion:**
   * Review answers as a group, explaining the reasoning behind each correct answer.
   * Highlight surprising results or common misconceptions.

**Activity 2: Group Exercise - Match Threats to Descriptions**

**Objective:** Help participants understand various cyber threats and how they work.  
**Time:** 20–25 minutes  
**Materials:**

* Pre-prepared cards or a digital board (e.g., Miro or Trello) with:
  + Threat names (e.g., phishing, malware, social engineering)
  + Descriptions/examples of the threats

**Instructions:**

1. **Preparation:**
   * Prepare two sets of cards:
     + **Threats**: Write the name of each threat on separate cards.
     + **Descriptions**: Write the corresponding description or example for each threat.
2. **Execution:**
   * Divide participants into small groups (3–5 people).
   * Distribute the cards randomly.
   * Ask each group to match threats with their correct descriptions.
   * Set a timer for 10–15 minutes.
3. **Discussion:**
   * Review the correct answers with the entire group.
   * Provide additional context or examples for each threat.

**Activity 3: Role-Play - Attackers vs. Defenders**

**Objective:** Practice identifying and countering social engineering tactics.  
**Time:** 30–40 minutes  
**Materials:**

* Pre-prepared role-play scenarios
* Role cards for "attackers" and "defenders"

**Instructions:**

1. **Preparation:**
   * Create 3–5 realistic scenarios involving social engineering. Examples:
     + *An attacker calls pretending to be IT support and asks for login credentials.*
     + *A suspicious USB drive is found in the office.*
     + *An email claims to be from HR requesting sensitive information.*
   * Write roles for attackers (e.g., impersonators, phishing email senders) and defenders (employees targeted in the scenario).
2. **Execution:**
   * Divide participants into pairs or small groups.
   * Assign roles and distribute scenario details.
   * Ask attackers to act out their role, attempting to trick defenders.
   * Defenders must respond using what they’ve learned about cybersecurity.
3. **Debrief:**
   * Discuss what worked and what didn’t for both attackers and defenders.
   * Highlight key lessons and effective defence strategies.

**Activity 4: Incident Response Simulation**

**Objective:** Practice the steps of identifying, reporting, and responding to a cybersecurity incident.  
**Time:** 40–50 minutes  
**Materials:**

* Incident scenarios (printed or displayed on a screen)
* Checklist of incident response steps

**Instructions:**

1. **Preparation:**
   * Prepare 2–3 incident scenarios. Examples:
     + *An employee clicks on a phishing link, and their device is compromised.*
     + *A ransomware message appears on a shared server.*
     + *Sensitive company files are leaked to the public.*
2. **Execution:**
   * Divide participants into teams.
   * Present a scenario to each team.
   * Ask teams to discuss and document how they would:
     + Identify the incident.
     + Report it to the appropriate team or authority.
     + Contain and mitigate the damage.
   * Allow 20–30 minutes for team discussions.
3. **Discussion:**
   * Each team presents their response plan.
   * Provide feedback and compare their plans with best practices.

**Activity 5: Password Strength Challenge**

**Objective:** Teach participants how to create and identify strong passwords.  
**Time:** 15–20 minutes  
**Materials:**

* Password examples (strong, weak, and average)
* Password manager recommendations

**Instructions:**

1. **Preparation:**
   * Prepare a list of password examples, including weak, average, and strong passwords. Examples:
     + Weak: password123
     + Average: MyDogSpot!
     + Strong: F!d3&k9#z2M
2. **Execution:**
   * Share the password examples with participants.
   * Ask them to rank the passwords from weakest to strongest and explain their reasoning.
   * Challenge them to create their own strong passwords using best practices.
3. **Discussion:**
   * Review their rankings and creations.
   * Provide tips on using password managers and enabling MFA.

**Activity 6: Remote Work Security Checklist**

**Objective:** Reinforce secure practices for remote work.  
**Time:** 20–25 minutes  
**Materials:**

* Checklist templates (digital or printed)
* Scenario examples of remote work risks

**Instructions:**

1. **Preparation:**
   * Create a checklist of secure remote work practices. Examples:
     + Use a VPN.
     + Avoid public Wi-Fi.
     + Lock devices when not in use.
2. **Execution:**
   * Distribute the checklist to participants.
   * Present remote work scenarios (e.g., working from a café, using a personal device for work).
   * Ask participants to identify which checklist items apply to each scenario.
3. **Discussion:**
   * Discuss their responses and highlight overlooked risks.