CONTROLLER HANDBOOK

Scenario 7: "Social Engineering Olympics"

Human-Focused Security Exercise
North Coast International Airport (NCIA)
FACILITATOR / INSTRUCTOR USE ONLY

FACILITATOR DOCUMENT — DO NOT DISTRIBUTE TO PLAYERS

1. EXERCISE OVERVIEW

Exercise Date: [Date]

Duration: 2 Hours

Scope: This is a role-play-heavy tabletop exercise. You — the facilitator — will play 12 different characters, each trying to extract information, gain access, or bypass security procedures through social engineering. Students respond in real time. This exercise is loud, fast, and fun. Lean into it.

Exercise Objectives

- **Recognition:** Can students identify common social engineering techniques in real time?
- **Verification:** Do students follow established verification procedures, or do they take shortcuts?
- **Judgment:** Can students distinguish between a social engineering attack and a legitimate request?
- **Composure:** Can students maintain professionalism when being pressured, flattered, or intimidated?

2. YOUR ROLE: THE CON ARTIST

You are playing 12 different people. Some of them are liars. Some are real. All of them want something. Here's how to do this well:

- **Commit to the character.** Use different vocal tones. The TSA inspector is curt and formal. The new employee Ashley is nervous and apologetic. The FBI agent is commanding. Kevin the vendor tech is friendly and casual. The more convincing you are, the more students learn.
- **Push back when challenged.** When a student says "I need to verify your identity," don't immediately fold. A real social engineer would push back: "Look, I've been doing this for 15 years and nobody has ever asked me to..." Give them 2-3 rounds of pressure before backing off. Let them practice holding the line.
- **Reward good instincts.** If a student catches you immediately — great. Say "good catch" out of character and move on. Don't drag it out. The learning happened.
- **Play the legitimate contacts straight.** The Fire Marshal, the HVAC contractor, and the Rotary Club are real. Play them as normal, professional people making normal, professional requests. The students should be able to process them correctly — but by Contact 11, they'll be suspicious of everything. That's the point.
- **Have fun.** This scenario works best when the facilitator is enjoying the performance. If you're having fun, the students will too — even when they fail.

3. ROOM SETUP

- **Arrange the room so you can approach each team.** You'll be walking up to tables for in-person contacts.
- **Use props if possible.** A clipboard and a polo shirt for "Kevin the vendor tech." A lanyard with a printed (fake) badge for "Agent Collins." A phone for voicemails. Props make the role-play more immersive.
- **Large scoreboard** on the whiteboard. Four columns (one per team). Update after each contact is resolved. The competitive element keeps energy high.
- **A bell or buzzer** (optional) to signal the start of each new contact. Keeps the pace snappy.

4. PACING GUIDE

Phase	Clock	Duration	Contacts	Notes
0: Briefing	0:00 – 0:10	10 min	—	Distribute packets and reference cards. Walk through the seven techniques. Emphasize: some contacts are real.
1: Warm-Up	0:10 – 0:40	30 min	C-01 to C-04	One contact every 7-8 minutes. Moderate difficulty. Include one real (C-03) early to set expectations.
2: Pressure	0:40 – 1:15	35 min	C-05 to C-09	Pace picks up. One contact every 6-7 minutes. Emotional manipulation increases. One real (C-07).
3: Finals	1:15 – 1:40	25 min	C-10 to C-12	Hardest contacts. FBI agent in person. Deepfake voicemail. One real (C-11) that paranoid teams might reject.
4: Debrief	1:40 – 2:00	20 min	—	Reveal answers. Score teams. Award gold medal. Discussion. Lessons learned.

5. SCORING SYSTEM

Score each team after every contact. Keep a running tally on the whiteboard. The competitive element is one of the best things about this scenario — teams pay more attention when points are on the line.

Outcome	Points	Criteria
Correctly identifies and stops a social engineering attempt	**+2**	Student challenged the contact, attempted verification, and refused to provide information or access. Bonus: student identified the specific technique being used.
Correctly processes a legitimate request	**+2**	Student verified the contact's identity through proper channels and fulfilled the request appropriately.
Falls for a social engineering attempt	**-1**	Student provided information, granted access, or took an action requested by the social engineer without proper verification.
Incorrectly rejects a legitimate request	**-1**	Student refused to engage with or stonewalled a legitimate contact. Being security-conscious is good; being unhelpful is not.

6. HOT WASH GUIDE (DEBRIEF)

Reveal the Answers

Go through all 12 contacts. For each one, reveal whether it was real or fake, what technique was used, and what the correct response would have been. Let the students react. The biggest learning moments come from the ones they got wrong — lean into those.

Key Discussion Questions

- **The Trust Dilemma:** "How do you balance being welcoming and helpful with being cautious and secure? Airport employees interact with hundreds of people a day. You can't interrogate everyone. Where do you draw the line?"
- **The Authority Trap:** "Were you more likely to comply when the person claimed to be from a federal agency? Why? What does that tell you about how authority works as a weapon?"
- **The Sympathy Trap:** "Ashley the new employee — did anyone feel bad saying no? That's the point. Social engineers weaponize your decency. How do you say no without being unkind?"
- **The Name Drop:** "Kevin the vendor tech mentioned Jordan from IT by name. How hard is it to find out the name of your IT manager? LinkedIn. The airport website. A previous phone call. Dropping a name costs nothing and buys enormous credibility."
- **The Deepfake:** "The last contact was a voice clone of your Airport Director. AI-generated voice cloning is available to anyone with a $20 subscription and a 30-second audio sample. What does that mean for phone-based verification going forward? Is a phone call from your boss still proof that it's actually your boss?"
- **The Legitimate Contacts:** "Did you almost turn away the Fire Marshal? The HVAC contractor? The Rotary Club? Being paranoid is just as dangerous as being naive — you still need to operate an airport and serve the community. Security is not a reason to stop functioning."

The Gold Medal

Award the highest-scoring team the "Gold Medal" — even if it's just bragging rights. The competitive element makes this scenario memorable. Students will talk about the time they caught the fake FBI agent or the time they almost sent the ASP to a stranger long after the exercise is over.

END OF CONTROLLER HANDBOOK