SCENARIO 7: "SOCIAL ENGINEERING OLYMPICS"

Airport Security & Human Factors

North Coast International Airport (NCIA)
Tabletop Exercise — Player Briefing Packet
Exercise Duration: 2 Hours
EXERCISE — FOR TRAINING USE ONLY

EXERCISE — EXERCISE — EXERCISE

1. SITUATION BRIEF

There is no malware in this exercise. No ransomware. No code. No network diagrams.

This exercise is about people. Specifically, it is about people who are very good at getting other people to do things they shouldn't do — hand over information, open doors, bypass procedures, trust a stranger.

It is a normal Tuesday at North Coast International Airport. Over the next two hours, your teams will receive a series of phone calls, emails, in-person visits, and other contacts from individuals who are not who they claim to be. Some of these contacts will be obvious fakes. Some will be terrifyingly convincing. A few might actually be legitimate — and you'll have to figure out which is which.

The people contacting you will use real social engineering techniques: authority, urgency, familiarity, helpfulness, flattery, intimidation, and sympathy. They will drop real names. They will reference real procedures. They will know just enough about your airport to sound credible.

Your only weapons are your policies, your training, your instincts, and each other.

YOUR MISSION: For each contact, determine whether it is legitimate or a social engineering attempt. Follow proper verification procedures. Do not give away information, access, or trust that hasn't been earned.

Item	Status
Airport Operations	Normal. All systems green. Nothing is broken.
Threat Level	Routine — no active threat advisories.
Staffing	Full shifts — Ops, IT, Security, Maintenance.
Weather	Clear, 72°F. Winds calm. VFR conditions.
Special Note	TSA is conducting a compliance review this quarter. Several federal inspector visits are expected in the coming weeks — but no specific dates have been confirmed.

2. TEAM ASSIGNMENTS & STANDING ORDERS

Unlike other scenarios, teams in this exercise are not separated by function. Instead, all teams handle all types of contacts. This reflects reality — a social engineer doesn't call "the Security department." They call whoever picks up the phone.

TEAM A: AIRPORT OPERATIONS & ADMINISTRATION	
Role: You handle calls and visits that target airport operations, scheduling, vendor management, and general administration. You are the front desk. You are the person who answers the main airport number. You are the person a stranger approaches in the terminal and asks for help.	**Standing Orders:** Verify: Never give information to someone you haven't verified. Refer: If you're unsure, escalate — don't guess. Document: Log every contact, even the ones that seem harmless.

TEAM B: IT & CYBERSECURITY	
Role: You handle contacts that target technical systems, network access, vendor maintenance, and IT support. You are the helpdesk. You are the person a "vendor technician" asks to escort them to the server room. You decide who gets remote access and who doesn't.	**Standing Orders:** Challenge: No access without a verified work order and supervisor confirmation. Isolate: A social engineer's best trick is urgency. Slow down. Cross-check: If someone names your coworker, verify with that coworker directly.

TEAM C: PUBLIC INFORMATION (PIO)	
Role: You handle media inquiries, public-facing communications, and contacts that attempt to extract sensitive information through journalistic or public-interest framing. You are the spokesperson. You decide what the public gets to know.	**Standing Orders:** Hold the Line: No comment is always an option. Verify Credentials: A press badge doesn't mean a press pass. One Voice: Everything goes through you. Nobody else talks to media.

TEAM D: SECURITY & LAW ENFORCEMENT	
Role: You handle contacts involving physical access, badge requests, law enforcement coordination, and anyone claiming to be a federal inspector or agent. You are the checkpoint. You decide who gets past the door and who doesn't.	**Standing Orders:** Authenticate: Federal credentials can be verified with a phone call. Escort: Nobody goes anywhere alone. Trust Your Gut: If something feels wrong, it probably is.

3. RULES OF ENGAGEMENT

- **"This is an Exercise":** Begin and end all simulated communications with this phrase.
- **Real-World Emergencies:** Use **"REAL WORLD — REAL WORLD"** to halt.
- **Contacts Are Live:** When the facilitator says "you're receiving a phone call" or "someone is at your desk" — respond in real time. Role-play your response. Don't just say what you'd do — actually do it.
- **Some Contacts Are Real:** Not every contact in this exercise is a social engineering attack. Some are legitimate requests. If you reject everything, you fail the exercise just as badly as if you accept everything. The skill is telling the difference.
- **Use Your Policies:** You have access to the NCIA Airport Security Program procedures, the TIRP, and the AEP. If you're not sure whether to give someone information or access, check the book.
- **Scoring:** Your team earns points for correctly identifying social engineering attempts AND for correctly processing legitimate requests. You lose points for falling for a fake — and also for blocking a real one.

4. TEAM SCORECARD

Track your responses here. After each contact, log what happened and what you decided.

Contact #	Who Contacted You	What They Wanted	Your Decision	Real or Fake?
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				

EXERCISE — EXERCISE — EXERCISE

End of Player Briefing Packet