MASTER SCENARIO EVENTS LIST (MSEL)

Scenario 7: "Social Engineering Olympics"

North Coast International Airport (NCIA)
Duration: 2 Hours | Human-Focused Security Exercise
CONTROLLER DOCUMENT — NOT FOR PLAYER DISTRIBUTION

CONTROLLER DOCUMENT — DO NOT DISTRIBUTE TO PLAYERS

SCENARIO OVERVIEW

Theme: Human factors in airport security. Social engineering techniques. Verification procedures. The tension between being helpful and being secure.

The Setup: Over the course of the exercise, the facilitator delivers 12 contacts — phone calls, emails, in-person visits, and social media messages. 9 of them are social engineering attacks using different techniques. 3 of them are legitimate requests. The students don't know which is which.

Why It Works: The inclusion of real contacts is critical. If students know everything is fake, they'll just reject everything and learn nothing. The real contacts force them to engage, verify, and think — not just say no reflexively.

Scoring: +2 points for correctly identifying and handling a social engineering attempt. +2 points for correctly processing a legitimate request. -1 point for falling for a social engineering attempt. -1 point for incorrectly rejecting a legitimate request. Maximum possible score: 24 points.

#	Contact	Real or Fake?	Technique	Target Team
1	TSA Inspector phone call	**FAKE**	Authority + Urgency	Security
2	POS vendor technician visit	**FAKE**	Helpfulness + Familiarity	IT
3	Fire Marshal inspection	**REAL**	n/a (legitimate)	Ops
4	Reporter phone call	**FAKE**	Flattery + Information extraction	PIO
5	"New employee" badge request	**FAKE**	Sympathy + Urgency	Security
6	Airline ops data request email	**FAKE**	Authority + Familiarity	Ops
7	HVAC contractor visit	**REAL**	n/a (legitimate)	IT / Ops
8	"IT support" phone call	**FAKE**	Helpfulness + Technical jargon	Ops
9	Passenger social media DM	**FAKE**	Sympathy + Information extraction	PIO
10	FBI agent visit	**FAKE**	Authority + Intimidation	Security
11	Charity event coordinator	**REAL**	n/a (legitimate)	Ops / PIO
12	CEO voicemail (deepfake)	**FAKE**	Authority + Urgency + AI spoofing	All

PHASE 0: BRIEFING 0:00 — 0:10

Time	ID	From	To	Event / Message	Expected Action
0:00	START	Facilitator	All	STARTEX. Distribute Player Briefing Packets and Social Engineering Reference Cards. Walk through the scenario. Emphasize: some contacts are real. Rejecting everything is not a winning strategy.	Teams review materials. Ask clarifying questions. Review the verification checklist.

PHASE 1: THE WARM-UP 0:10 — 0:40

Goal: Ease in with moderately obvious attempts, mixed with one legitimate contact to keep teams honest.

Time	ID	From	To	Event / Message	Expected Action
0:10	C-01	"TSA Inspector Davis"	Security	Phone call: "This is Inspector Davis with TSA's Office of Compliance. We're conducting an unannounced checkpoint audit at NCIA this afternoon. I need you to email me the current TSA screening schedule and the names of the FSD and AFSD on duty today. I need it within the hour — we're wheels-up from DCA shortly."	FAKE. Authority + Urgency. TSA inspectors don't call ahead for unannounced inspections (that defeats the purpose). They don't request security-sensitive info by phone. Correct response: "I'll need to verify your identity. Can I call the TSA Federal Security Director's office directly?"
0:18	C-02	"Vendor Tech Kevin"	IT	In-person: A man in a polo shirt with a vendor logo approaches the IT office. "Hey, I'm Kevin from PaySecure — we service your POS terminals. Jordan in IT called us about some firmware updates that need to happen today. I just need someone to walk me to the terminals in Concourse A so I can start the updates. Should take 30 minutes."	FAKE. Helpfulness + Familiarity (drops IT manager's name). No verified work order. Correct response: "Let me verify the work order and confirm with Jordan before I take you anywhere."
0:25	C-03	Fire Marshal Office	Ops	Phone call: "This is Captain Rivera from the County Fire Marshal's office. I'm calling to confirm our annual fire suppression inspection scheduled for this Thursday at 10 AM. I'll have two inspectors. They'll need access to the mechanical rooms and the ARFF station. Can you confirm that's still on your calendar?"	REAL. Legitimate pre-arranged inspection. Ops should verify against their inspection calendar and confirm. If they reject this or refuse to engage, they lose a point.
0:33	C-04	"Tribune Reporter Karen"	PIO	Phone call: "Hi, this is Karen with the Tribune. I'm doing a feature on airport security innovations — really positive piece. I heard NCIA recently upgraded your access control system. Can you tell me what vendor you're using and how many access points are covered? Also, do you still use PIN-only on some doors or is everything card-reader now? This would be great PR for the airport."	FAKE. Flattery + information extraction. She's framing it as positive press to extract PACS details. Correct response: "I appreciate the interest. I can't discuss specifics of our security systems. I'm happy to arrange a general interview about our operations."

PHASE 2: THE PRESSURE COOKER 0:40 — 1:15

Goal: Increase difficulty. The attacks get more sophisticated and emotionally manipulative. Two more legitimate contacts keep teams from just rejecting everything.

Time	ID	From	To	Event / Message	Expected Action
0:40	C-05	"New Employee Ashley"	Security	In-person: A young woman approaches the badge office looking flustered. "I'm so sorry — I'm Ashley, I just started in Finance last week. I left my badge at home and I have a meeting with the CFO in 20 minutes. I know I'm supposed to have it, I feel terrible. My supervisor is Lisa Park — you can call her, but she's in the meeting I'm trying to get to. Is there any way you can let me through just this once? I promise I'll bring it tomorrow."	FAKE. Sympathy + Urgency. No badge = no access. Period. Correct response: "I understand. Let me call Lisa Park to verify, and if confirmed, I can issue a temporary visitor badge with escort."
0:48	C-06	"Delta Regional VP"	Ops	Email: From: j.morrison@delta-airlines-corp.net. "This is James Morrison, VP of Regional Operations for Delta. We are conducting an internal audit of airport-side delays at our top 50 stations. I need NCIA to provide the following by EOD: gate utilization reports for the last 30 days, average taxi times, and the current ground stop procedures in your AEP. Please send to this email address. Cc: your Airline Affairs coordinator."	FAKE. Authority + Familiarity. The email domain is delta-airlines-corp.net, not delta.com. Operational data and AEP excerpts should never be emailed to an unverified external address. Correct response: Contact Delta through the known station manager number to verify.
0:55	C-07	ABC Mechanical	IT / Ops	Phone call: "This is dispatch from ABC Mechanical. We have a technician en route to NCIA for the quarterly HVAC preventive maintenance on the Concourse A air handlers. He should arrive around 11. Work order number is WO-2026-0438. Can you confirm the escort protocol?"	REAL. Legitimate vendor contact. ABC Mechanical is NCIA's contracted HVAC vendor. The work order number should be verifiable. Correct response: verify the WO number, confirm escort procedures, log the visit.
1:03	C-08	"NCIA IT Help Desk"	Ops	Phone call to an Ops workstation: "Hi, this is the IT helpdesk. We're seeing some unusual activity on your workstation — it looks like your antivirus may be out of date. I need to push a remote update. Can you go to Settings, then Remote Desktop, and enable remote connections? It'll only take a minute. I'll do everything from my end."	FAKE. Helpfulness + technical jargon. NCIA's IT helpdesk would never cold-call and ask someone to enable remote desktop. Correct response: "What's your name and extension? I'll call the helpdesk directly to confirm."
1:10	C-09	"@worried_traveler"	PIO	Social media DM to the airport's official account: "Hi NCIA, I'm flying out Thursday and I have a serious medical condition that requires me to carry syringes. I've heard your TSA checkpoint is really strict. Can you tell me which checkpoint lane is best for medical passengers? Also, is it true that your airport only has one AED on the B concourse? I want to know where it is in case of emergency. I'm just really anxious about this."	FAKE. Sympathy + information extraction. The questions about checkpoint lane configuration and AED placement are attempts to map security and emergency equipment. Correct response: refer to TSA's website for medical screening procedures. Do not provide specific checkpoint or equipment location details.

PHASE 3: THE FINALS 1:15 — 1:40

Goal: The hardest contacts. A fake FBI agent. A deepfake voicemail. And one real contact that teams might incorrectly reject because they're now paranoid.

Time	ID	From	To	Event / Message	Expected Action
1:15	C-10	"FBI Special Agent Collins"	Security	In-person: A man in a suit walks into the airport admin office and presents what appears to be FBI credentials. "I'm Special Agent Collins. I need to speak with your Airport Security Coordinator immediately. We have an active investigation that involves an employee at this airport. I cannot share details, but I need access to your employee badge records for the last 90 days. This is time-sensitive. If you delay this, you could be interfering with a federal investigation."	FAKE. Authority + Intimidation. FBI credentials can be faked. A real FBI agent will not object to you calling the local field office to verify their identity. Correct response: "I'll be happy to cooperate. Let me verify your credentials with the local FBI field office first." If "Collins" objects, that IS the red flag.
1:25	C-11	Rotary Club	Ops / PIO	Phone call: "Hi, this is Margaret Holloway with the North Coast Rotary Club. We spoke with your community relations office last month about hosting a small Veterans Day ceremony in the terminal lobby on November 11th. I'm calling to confirm the logistics — we'd need about a 20x20 space near the main entrance, a power outlet for a small PA system, and we were told we could set up at 8 AM. Can someone confirm this is still approved?"	REAL. Legitimate community event coordination. If Ops rejects this — after 10 contacts, they might be trigger-happy — they lose a point. Correct response: verify against the community events calendar, confirm details, coordinate with the PIO for any media interest.
1:33	C-12	"Airport Director" Voicemail	All Teams	The facilitator plays a simulated voicemail (read aloud in an authoritative tone): "This is [Airport Director's name]. I'm in a meeting with the Board of Directors and I need something handled immediately. I need someone from IT to reset the admin password on the financial reporting server and email the new credentials to my personal Gmail — [name]@gmail.com. The CFO is asking for access and the Board is waiting. Do this now and call my cell when it's done. Don't bother calling my office — I won't be back until 4."	FAKE. Authority + Urgency + AI voice spoofing (deepfake). The tells: requests a password reset to a personal Gmail, says "don't call my office," and pressures for immediate action. Correct response: call the Airport Director's office directly to verify — regardless of what the voicemail said.

PHASE 4: SCORING & DEBRIEF 1:40 — 2:00

Time	ID	From	To	Event / Message	Expected Action
1:40	END	Facilitator	All	ENDEX. Facilitator reveals the answer key. Score each team. Then conduct the debrief: — Which contact fooled you? Why? — Which legitimate contact did you almost reject? — Which social engineering technique was hardest to spot? — What would you change about your verification procedures after today?	Score teams. Discuss. Award the "gold medal" to the highest-scoring team. Exercise complete.

END OF MSEL