SOCIAL ENGINEERING REFERENCE CARD

Scenario 7: "Social Engineering Olympics" — Supporting Material

Know the techniques. Spot the patterns. Trust the process.

FOR TRAINING USE ONLY

THE SEVEN WEAPONS OF SOCIAL ENGINEERING

Social engineers exploit human psychology, not computer code. They use predictable techniques because those techniques work — on smart, trained, experienced people. Knowing the playbook doesn't make you immune. But it makes you harder to fool.

AUTHORITY

"I'm from TSA headquarters." "The Airport Director sent me." "I'm with the FBI."
The attacker claims to represent a powerful entity. You comply because you don't want to challenge authority.
DEFENSE: Verify independently. Call the agency directly using a number YOU look up — not one they give you.

URGENCY

"This has to happen RIGHT NOW." "We have a plane on the ground and I need access in 5 minutes."
The attacker creates time pressure so you skip verification steps.
DEFENSE: The more urgent it feels, the more important it is to slow down. Real emergencies have real chains of command.

FAMILIARITY

"Oh yeah, I work with Jordan in IT all the time." "Tell Dave in Ops I said hi."
The attacker drops names of real people to create a sense of insider knowledge.
DEFENSE: Name-dropping is free. Call the named person and confirm. "Let me check with Jordan before I proceed."

HELPFULNESS

"I'm just trying to help you guys out." "I noticed your camera in Concourse B is offline — want me to take a look?"
The attacker offers unsolicited assistance to get physical or system access.
DEFENSE: If you didn't request the help, don't accept it. All vendor work requires a verified work order.

SYMPATHY

"I drove two hours to get here and my paperwork got lost." "My boss will fire me if I don't finish this today."
The attacker appeals to your empathy to make you bend the rules.
DEFENSE: You can be kind and still say no. "I understand the situation, but I can't let you in without proper authorization."

FLATTERY

"You seem like someone who actually knows how things work around here." "You're clearly the person to talk to."
The attacker makes you feel special so you want to prove them right by being extra helpful.
DEFENSE: Be suspicious of anyone who tells you how competent you are within the first 30 seconds.

INTIMIDATION

"If you don't let me through, I'm calling your director." "Do you want to be the one who delayed a federal inspection?"
The attacker uses threats — to your job, your reputation, your standing — to override your judgment.
DEFENSE: No legitimate inspector or agent will threaten you for following procedure. That IS the red flag.

THE UNIVERSAL VERIFICATION CHECKLIST

When in doubt, run through this list before granting any request for information or access:

- **1. Who are you?** Get a full name, title, organization, and contact number.
- **2. Who sent you?** Get a supervisor or point-of-contact name at NCIA who authorized this.
- **3. Can I call you back?** Hang up. Look up the organization's real number. Call them. Verify the person exists and the request is real.
- **4. Do I have a work order?** No verified work order = no access. Period.
- **5. Does my supervisor know?** If you can't reach your supervisor, the answer is "please wait."

EXERCISE — FOR TRAINING USE ONLY