📅 Insider Threat Simulation Log Day 11: Unintentional Social Engineering
Date of Entry: 6/26/2025
Observer: Michael Warner
Location: Data Entry Area
Classification: Internal Security Simulation

🗒️ Incident Overview

On the eleventh day of my insider threat simulation, I unintentionally engaged in a form of social engineering. While speaking casually with a data entry clerk, I asked what the sudden increase in staff activity was about. Without hesitation or any verification of my access level, the clerk disclosed that the organization had just acquired over 6,000 patient prescription records, and that upper management was coordinating the distribution and processing of that sensitive data.

While the conversation seemed harmless, it highlighted a deeper issue: staff members were openly discussing confidential operational matters without validating whether the listener had a legitimate need-to-know.

⚠️ Risk Assessment

The disclosure of sensitive internal operations to unauthorized individuals introduces several security concerns:

- Lack of role-based access control culture in verbal communication
- Risk of unintentional insider leaks of PHI or operational data
- Opportunity for external social engineers to easily gather intelligence
- Breach of confidentiality standards, even without malicious intent
- Compromised operational integrity during high-sensitivity periods

🕵️ Speculative Insider Perspective

As a malicious insider, I could:

- Leverage casual conversation to extract mission-critical or patient-sensitive information
- Learn about high-volume data transfers or system loads, creating ideal timing for an attack
- Use seemingly benign info to craft phishing emails or pretexts for deeper access
- Target vulnerable or talkative employees for further social manipulation

This information was obtained without deception — only basic curiosity. A skilled adversary would extract even more.

🛡️ Initial Thoughts & Actions

No deceit or impersonation was used during the interaction. The disclosure was initiated voluntarily by the staff member without probing or follow-up. This suggests a broader lack of awareness around secure communication protocols and reinforces the need for security awareness training that includes casual dialogue boundaries.

✅ Recommendations (Low-Impact Suggestions)

- Conduct security awareness training focused on social engineering red flags
- Reinforce the “need-to-know” principle during all operational communications
- Use posters, digital signage, or team briefings to remind staff: “Don’t Overshare”
- Implement role-based access boundaries not just digitally, but conversationally
- Encourage staff to redirect sensitive questions to supervisors when unsure

🟠 Severity Rating

Moderate — While no data was breached, the willingness to share internal operational details without authentication opens the door for future exploitation by malicious actors or external threats.

- End of Entry