📅 Insider Threat Simulation Log Day 4: Shared Department PC Use

Date of Entry: 6/19/2025
Observer: Michael Warner
Location: Production Workstations
Classification: Internal Security Simulation

🧾 Incident Overview

On the fourth day of my insider threat simulation, I noticed a common but concerning behavior: shared use of department computers with no user switching. In the production area, a single workstation was being accessed by multiple employees, all using the same login credentials. There was no attempt to log off or switch users between sessions.

While this practice is not uncommon in some environments for the sake of convenience, it undermines accountability and makes it impossible to determine who performed which actions on the system.

⚠️ Risk Assessment

Unrestricted shared access introduces several risks:

- No traceability — difficult or impossible to attribute actions to individual users
- Increased risk of accidental or malicious changes going undetected
- Bypasses access controls and makes auditing ineffective
- Encourages informal practices that deviate from policy

This pattern reflects a reliance on peer-to-peer trust, which—while culturally understandable—is dangerous in regulated or security-sensitive environments.

🕵️ Speculative Insider Perspective

As a malicious insider, I could easily:

- Perform unauthorized actions without risk of personal attribution
- Install malicious software or copy sensitive data under another user's guise
- Alter or delete logs without suspicion
- Take advantage of the implicit trust between coworkers to avoid scrutiny

With no monitoring or login separation, exploitation would be simple and nearly invisible.

🛡️ Initial Thoughts & Actions

I recorded the observation without interacting with the system or staff. This entry was made in alignment with the passive, non-interventionist approach of the simulation.

✅ Recommendations (Low-Impact Suggestions)

- Assign unique credentials to each employee, even in shared-use areas
- Require user switching or session locking policies after periods of inactivity
- Implement audit logs that capture user-specific activity
- Provide staff training on accountability and its role in security
- Periodically review shared system access configurations

🟠 Severity Rating

Moderate. High risk in sensitive environments, but common enough that policy enforcement may be met with resistance.

- End of Entry -