📅 Insider Threat Simulation Log Day 3: Passwords on Sticky Notes
Date of Entry: 6/18/2025
Observer: Michael Warner
Location: Production & Data Entry Workstations
Classification: Internal Security Simulation

🗒️ Incident Overview

On the third day of my insider threat simulation, I observed a recurring and concerning behavior: passwords written on sticky notes and placed in visible locations near active workstations. These were found throughout the building — primarily in the production area, but also in several data entry stations.

Sticky notes were often affixed to the bottom edges of monitors, desk drawers, or pinned near keyboards. In several cases, the usernames and passwords appeared to be plaintext login credentials, likely for internal systems. Such practices severely weaken authentication controls and directly compromise system confidentiality.

⚠️ Risk Assessment

This reflects a lack of user training and poor enforcement of credential handling policies. Publicly visible credentials introduce several risks:

● Anyone — including visitors or unauthorized personnel — can observe or photograph credentials
● Stolen credentials enable unauthorized system access
● Creates a false sense of security and normalizes poor cybersecurity hygiene
● Enables lateral movement if reused across multiple systems

🕵️ Speculative Insider Perspective

There was no deterrence or monitoring around these stations, making exploitation extremely low-risk. As a malicious insider, this would be a prime target. With minimal effort, I could:

● Log the credentials and use them after hours
● Use the credentials to elevate access or pivot into more sensitive systems
● Capture login patterns and build a profile of user behavior
● Photograph credentials and share them externally

🛡️ Initial Thoughts & Actions

I documented the location and content format of these sticky notes without removing or altering them. No system access was attempted, and no individuals were confronted. This entry was logged discretely in accordance with the simulation's non-disruptive policy.

✅ Recommendations (Low-Impact Suggestions)

- Conduct a facility-wide sweep for visible credentials
- Provide password management training during onboarding and quarterly refreshers
- Enforce a policy that prohibits writing down passwords in visible areas
- Recommend use of secure password managers where applicable
- Consider desk audits or surprise inspections

🟠 Severity Rating

Moderate, with high exploitation potential if credentials grant elevated access or are reused system-wide.

- End of Entry -