USB Baiting Activity: Parking Lot USB Exercise

# Contents

The USB drive contains both personal and work-related files. Among the contents are family and pet photos, a new hire letter, and an employee shift schedule. This indicates the drive holds sensitive information such as personally identifiable information (PII) and internal employee data.

# Attacker Mindset

An attacker could use the files to gather intelligence on Jorge or other hospital staff. The new hire letter and shift schedule may reveal employment patterns, names, and contact info. The entire event could be staged to lure an employee into plugging in the USB, creating a backdoor into the hospital’s network.

# Risk Analysis

USB baiting attacks can deliver malicious software such as keyloggers, ransomware, or remote access tools. If another employee had found and used the drive on a network-connected system, it could have led to a severe data breach. Sensitive information like employee schedules could aid in social engineering attacks. To mitigate this risk, organizations should implement technical controls like disabling USB ports or using endpoint protection software, and managerial controls like strict security policies and employee awareness training. Physical controls like signage and secure device storage can also help reduce the chance of accidental use.