

Contents

The USB drive contains both personal and work-related files, including family and pet photos, a new hire letter, and an employee shift schedule. The presence of personally identifiable information (PII) and sensitive work documents makes this device a potential security risk. Storing personal files alongside work files is unsafe, as it increases the risk of unauthorized access to company data if the drive is lost or stolen.

Attacker Mindset

An attacker could use the personal files to craft phishing attacks against Jorge, his colleagues, or even his family members. The work files, such as employee schedules, could provide insights into staffing patterns, making the hospital more vulnerable to social engineering or physical security breaches. If the USB drive was intentionally planted, it may have been a baiting attempt to gain access to the hospital's internal systems.

Risk Analysis

USB baiting attacks often involve malware, such as keyloggers, ransomware, or remote access trojans (RATs). If an infected device were plugged into a company workstation, it could compromise the entire network. To mitigate such risks, organizations should implement technical controls like endpoint detection software, disable USB ports on sensitive systems, and use virtualized environments for testing. Operational policies should enforce strict separation of personal and work data, while security awareness training can educate employees on the dangers of plugging in unknown USB drives.