Scenario

Review the following scenario. Then complete the step-by-step instructions.

You are part of the security team at **Rhetorical Hospital** and arrive to work one morning. On the ground of the parking lot, you find a USB stick with the hospital's logo printed on it. There’s no one else around who might have dropped it, so you decide to pick it up out of curiosity.

You bring the USB drive back to your office where the team has virtualization software installed on a workstation. Virtualization software can be used for this very purpose because it’s one of the only ways to safely investigate an unfamiliar USB stick. The software works by running a simulated instance of the computer on the same workstation. This simulation isn’t connected to other files or networks, so the USB drive can’t affect other systems if it happens to be infected with malicious software.

Parking lot USB exercise

Contents	In the USB device store PII information is related to ‘Jorge’. - Personal information about vacation, wedding - Organisational information about budget, shifts, hires
Attacker mindset	The excel files can provide an attacker information about other people from Rhetorical Hospital. Also, this information could be used to trick Jorge. Malicious actor could use these knowledge to email phishing.

Risk analysis	Promoting employees with this type of attack (usb baiting). Disable Autorun of external devices on workstations. Keep personal and business USB drives separate. Use passwords and encryption on your USB drive