Scenario: MALWARE

Details:

A new employee in Human Resources reported that their desktop computer was "acting funny." When the IT Department does some troubleshooting, they discover malware on the employee's computer.

When IT talks to the employee about how the malware may have been introduced onto the computer, the employee was unsure. The employee did mention that they found a "beat-up" old USB Flash Drive in the parking lot they thought might be good to transport files; so, they plugged it into their computer's USB port. IT concluded that the USB Flash Drive was the most likely source of the malware and was inadvertently introduced by the employee.

Notes:

- What are some precautions you can take to guard against malware being introduced into company devices and networks?
- Which policies should include guidance on employee use of USB Flash Drives?
- As the USB Flash Drive originated in the parking lot, what are some investigative steps the company can take to determine who dropped it?
- Which roles should be involved in discussing this issue?