Scenario: PHISHING
Inject 3

Role: ***INFORMATION TECHNOLOGY***

Detail:

- The IT team discovers a recent email containing a suspicious URL that was clicked on by an Organization employee.
- This caused several small binary files to be downloaded onto the employee's computer.
- These files created an encrypted connection from the computer to a remote system.
- That connection remained active until the computer was quarantined and removed from the network.
- The file signature of a file found on the computer matches a newly-reported keylogger and ransomware variant.

What do you do with this information?

CISA Cybersecurity Performance Goal:
Email Security (2.M)

MassCyberCenter.org