Something Suspicious Happening?

Escalaro

Suspicious Activity?

- As soon as possible:
- Switch to Airplane Mode if possible
- Disconnect from ALL networks.

User Containment

Supervisor

- Provide a brief on incident.
- Decide who the "appropriate everybody" is for the next step.
- Any other immediate actions to take?
- Inform the "appropriate everybody" that was determined with the Supervisor.
- Start taking notes about what happened.
- Then notify the ISO

Everybody

Information Security Officer

escalato

- Inform of incident and steps taken so far.
- Investigate and decide whether to escalate to Incident Response Team (Is customer information or money involved?)
- Start logging Indicators of Compromise.

- Decide on:
- Mitigation options
- Determine whether to involve the insurance company.
- Decide what, if any, External Entities need to be alerted.

Incident Response Team

External Entities

- Board of Directors
- Regulators
- Law Enforcement
- Other Authorities
- Customers
- Media

Escalate



Alert

Be Sure to Broadcast Awareness Properly