Suspicious Message Triage

Secondary, higher ed, professional | Runbook | 30-60 minutes

Before class: This is an instructor preparation runbook. Assemble the fictional scenarios, messages, or data it specifies before use; it does not provision a lab or include a ready-made dataset.

Lab ID: MSG-TRIAGE-01 Outcome: Analyze fictional messages and select safe verification and reporting actions. Environment: Printed or offline digital evidence set; no live links. Time: 30-60 minutes.

Authorization and Boundaries

- Only instructor-supplied fictional messages may be analyzed.
- Learners do not click, reply, download, call, scan, or enter information.
- No real person or organization is impersonated.
- If a real suspicious message is discovered, stop the exercise and use the institution's reporting process.

Instructor Preparation

1. Create or review three to six messages.
2. Confirm every link and contact is inert or fictional.
3. Include at least one legitimate but unusual message and one ambiguous message.
4. Print or distribute the evidence record.
5. Verify the reporting flow used in the course.

Expected Learner Evidence

- Context, identity, action, pressure, destination, and data analysis
- Independent verification method
- Reporting decision
- Response after accidental exposure
- Statement of unresolved uncertainty

Reset

Collect or delete learner copies if required, remove annotations containing personal information, restore the clean evidence set, and record confusing cues for revision.

Common Failure Modes

- Treating spelling errors as the primary indicator
- Assuming familiar branding proves identity
- Using contact information contained in the suspicious message
- Declaring a message malicious without sufficient evidence
- Failing to describe action after credentials are exposed

Source and use

The Complete Cybersecurity Educator, Dr. Jason Edwards. Editable companion - Runbook 1 - Suspicious Message Triage.

Sharing and reuse: Please do not resell this resource. You may repost or share it with other educators. Please leave the Bare Metal Cyber Educators Hub URL below intact. Use fictional or appropriately authorized data where applicable.

Read online: https://educate.baremetalcyber.com/resources/suspicious-message-triage/