Identity Lifecycle Map

Grades 7-8 | Lesson | 55 minutes

Before class: Prepare the fictional school-club account scenario, lifecycle cards, and mapping worksheet listed below. This download supplies the teaching plan, not a complete card deck.

Time: 55 minutes Outcome: Learners will map proofing, provisioning, authentication, authorization, review, change, recovery, and deprovisioning for a fictional account.

Materials

- Identity lifecycle cards
- Fictional school-club account scenario
- Mapping worksheet

Safety and Privacy

Use a fictional account and invented roles. Do not review real school directory information or account settings.

Activity

Teams arrange lifecycle cards for a new student club member. The scenario then changes: the learner becomes treasurer, loses a device, and later leaves the club. Teams update access and identify risks at each transition.

Evidence

An annotated lifecycle map showing who approves access, how authentication is protected, how access is reviewed, and how sessions and credentials are removed.

Debrief

- Why can an unused account remain dangerous?
- How can recovery become an alternate attack path?
- What evidence should exist after access changes?

Source and use

The Complete Cybersecurity Educator, Dr. Jason Edwards. Editable companion - Lesson 3.1 - Identity Lifecycle Map.

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/identity-lifecycle-map/

Social Engineering Verification Drill

Grades 7-8 | Lesson | 50 minutes

Before class: Prepare announced role cards, request cards, and a verification worksheet. Do not run surprise deception against real students.

Time: 50 minutes Outcome: Learners will respond to pressure-based requests using independent verification and documented reporting.

Materials

- Role cards
- Request cards
- Verification-plan worksheet

Safety and Privacy

Do not target real students with surprise deception. All requests are announced classroom simulations.

Activity

Learners rotate through roles: requester, recipient, verifier, and observer. Request cards include authority, urgency, curiosity, fear, and reward. The recipient must avoid using contact details contained in the request and select a separately trusted verification channel.

Evidence

The observer records pressure technique, recipient action, verification path, and one improvement.

Debrief

- Which pressure technique was hardest to resist?
- Why can helpfulness create risk?
- How should organizations design reporting so people do not feel blamed?

Source and use

The Complete Cybersecurity Educator, Dr. Jason Edwards. Editable companion - Lesson 3.2 - Social Engineering Verification Drill.

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/social-engineering-verification-drill/

Secure Configuration Review

Grades 7-8 | Lesson | 60 minutes

Before class: Prepare an invented configuration sheet using the six example issues in the plan; add risk-ranking cards and a recommendation template.

Time: 60 minutes Outcome: Learners will identify and prioritize security weaknesses in a sanitized configuration excerpt.

Materials

- Fictional configuration sheet
- Risk-ranking cards
- Recommendation template

Safety and Privacy

No live system access is required. The configuration is invented and contains no operational target information.

Activity

The fictional configuration includes:

- Shared administrator account
- Unused account still active
- Logging disabled for account changes
- Overly broad access rule
- Unprotected backup share
- Missing owner and review date

Teams identify evidence, risk, recommendation, operational consequence, test, and rollback for each issue.

Assessment

Use accuracy, prioritization, consideration of operational impact, and verification plan.

Debrief

- Why can a technically stronger setting still create operational risk?
- What should happen before a configuration is changed?
- Which finding should be addressed first, and what evidence supports that decision?

Source and use

The Complete Cybersecurity Educator, Dr. Jason Edwards. Editable companion - Lesson 3.3 - Secure Configuration Review.

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/secure-configuration-review/