Timestamp & Context:

- From who: John Smith
- Time & Date: 2025-09-11T13:45:00Z
- Automated alert triggered when an unauthenticated email message was delivered
- Authorization granted to inspect IdP logs around 15 minutes of the delivery time and examine the email under minimum-necessary evidence policy

Authorization:

- Incident Manager: John Smith
- Scope: IdP logs (13:30-14:00Z window) and suspicious email.

Actions Taken:

- Export and examine the log in the specific time window for anything suspicious
- Safely obtain the suspicious email from the quarantined Mailbox
- Open the suspicious email in read only mode

Evidence Captured:

- SHA256: 23f9985b71f3b714172addc83c0158a00cf99193f7cac42c52b6aeefb6fdf48a (Website)
- SHA256: b2e70976a832a7a5c1ef979042a3cdac4cbea710dbcd0e69eb405f2d258c2346 (Email)
- Minimum Necessary: 30 minute instance of logging

Chain of Custody:

- The information will be secured in a repository labeled "/secured_evidence/hc-1066"
- Every time the information is accessed, the repository will log who visited it and for how long
- As of 2025-09-11T14:30Z, Only the incident Manager John Smith and I have had access to these files.

Redaction:

- Removed message header fields
- Reset passwords for all students and/or MFA's

Next Step recommendation:

- Push to containment team to verify spoofing domain
- Phishing campaign should be assessed and pushed to prevent future incidents
- Alert Sam Rivera and the IT communications team per policy.