Incident & Evidence Note

Incident #: HC-IR-1066

Timestamp & Context (UTC):

- 2025-09-11T13:45:00Z Incident Manager John Smith declared an incident and opened ticket HC-IR-1066 after an automated alert flagged a phishing email delivered to student Sam Rivera at 13:07 UTC.

Authorization:

- John Smith (Incident Manager) approved collection of the suspicious email (.eml) and inspection of IdP sign-in logs for Sam Rivera within a ±15-minute window around 13:07 UTC. No other assets or data were authorized.

Actions Taken:

- Exported the suspicious email as a raw `.eml` file with headers and body intact.
- Filtered the IdP log to include only Sam Rivera's entries from 12:52–13:22 UTC (±15 minutes).
- Calculated SHA-256 checksums for both the `.eml` file and the filtered `.csv` log.
- Logged evidence inventory and chain of custody at the time of collection.

Evidence Captured (Minimal Necessary):

- **EV-001:** `Phish_SamRivera_20250911.eml`
    - SHA-256: `b2e70976a832a7a5c1ef979042a3cdac4cbea710dbcd0e69eb405f2d258c2346`
    - Why: Contains spoofed Blackboard email with credential-harvest HTML attachment; shows DMARC fail and spoofing indicators.

- **EV-002:** `IdP_SamRivera_20250911_1252-1322.csv`
    - SHA-256: `40624354322f9014ab638dcbe00a5c3eb586df18b72c47945ac72e9b39b1b158`
    - Why: Narrowed to Sam Rivera's IdP log entries ±15 minutes of phishing email; confirms password-only attempts within scope while excluding unrelated users.

Chain of Custody:

Time (UTC)	Item ID	From → To	Location	Action/Purpose	Signature/ID
13:50Z	EV-001	Collector → Evidence Share	`/evidence/HC-IR-1066/Phish_SamRivera_20250911.eml`	Intake + SHA-256 (`b2e70976a832a7a5c1ef979042a3cdac4cbea710dbcd0e69eb405f2d258c2346`)	CH
13:55Z	EV-002	Collector → Evidence Share	`/evidence/HC-IR-1066/IdP_SamRivera_20250911_1252-1322.csv`	Intake + SHA-256 (`40624354322f9014ab638dcbe00a5c3eb586df18b72c47945ac72e9b39b1b158`)	CH

Redaction:

- Filtered the IdP log to include only Sam Rivera's sign-in entries within the approved ±15 minute window (12:52–13:22 UTC).
- Removed all other user data to avoid exposing unrelated accounts.
- Did not include any passwords, tokens, or credentials in this note.
- Retained original unfiltered log securely in evidence storage for reference if later approved.

Next Step Recommendation:

- Recommend soft containment: reset Sam Rivera's password, revoke active sessions/tokens, and block the suspicious sender domain `*.blackboard-mail.center` at the mail gateway. This preserves account security and limits further phish attempts while minimizing disruption to other services. Handoff to

the IdP Manager and Email Administration team for follow-up monitoring and recovery actions.