INCIDENT RESPONSE REPORT

Title: Account Hijack Attempt and Credential Exposure - Simulated Tabletop Exercise

Author: Brandon Jones

Date: July 25, 2025

Exercise Type: Personal Cybersecurity Tabletop (Simulated Real-World Incident)

Objective: Demonstrate individual response capability to an identity-based cyberattack during job search activity.

1. Executive Summary

This tabletop simulation modeled a realistic cyberattack against my digital life as a student and job seeker in cybersecurity. The incident involved a targeted phishing email, unauthorized account access attempts, and evidence of password reuse exploitation. My response focused on containment, verification, recovery, and post-incident hardening across multiple systems.

2. Timeline of Events

8:05 AM - Gmail alert: Suspicious sign-in attempt blocked from Russia.

8:10 AM - Received a spoofed email mimicking university IT asking for urgent password reset.

8:20 AM - Coursera account inaccessible; password reset email confirmed unauthorized change.

8:30 AM - Observed unfamiliar IP access attempt on student portal (New York).

9:00 AM - Initiated password resets on core accounts through official logins, not email links.

9:30 AM - Contacted university IT and Coursera support via official channels.

10:00 AM - Investigated email exposure via HaveIBeenPwned; found compromised job board accou

11:00 AM - Began hardening long-term digital security posture.

3. Impact Summary

Incident Response Report

- Accounts Targeted: Gmail, Coursera, university student portal, Apple ID

- Data at Risk: Educational records, certification progress, job application details

- Attack Vector: Credential stuffing from breached job board account; phishing attempt

- Response Time: Less than 1 hour to initiate containment

4. Incident Response Actions

Containment:

- Logged in via official portals to manually verify activity.

- Reset passwords for affected and related accounts using unique, complex credentials.

- Did not engage with phishing email; flagged as suspicious.

Eradication & Recovery:

- Verified recovery email settings and MFA on all major accounts.

- Notified university IT and Coursera to begin recovery and monitoring processes.

- Audited browser-saved credentials and removed weak/reused entries.

Lessons Learned:

- Password reuse significantly increases blast radius of even low-level breaches.

- Phishing can be extremely convincing when it mimics known entities.

- Time to detection and response directly reduces risk of deeper compromise.

5. Post-Incident Improvements

- Adopted a password manager (e.g., Bitwarden)

- Established a 90-day password rotation policy for key accounts

- Subscribed to HaveIBeenPwned breach monitoring
- Enabled recovery codes and backup MFA methods
- Began using a VPN on untrusted networks
- Created a personal digital hygiene checklist for monthly review

6. Conclusion

This exercise highlighted the real-world risks faced by cybersecurity students and professionals alike. By responding quickly, verifying all communications, and implementing best practices post-incident, I successfully contained the threat and strengthened my long-term defenses.