PART ONE: Scenario Name: Operation Identity Check

Objective:

To enhance the TSU Helpdesk team's vigilance and proficiency in identifying and responding to fraudulent account creation requests, particularly those involving advanced tactics like Business Email Compromise (BEC) and AI-generated fake identities (DeepFakes).

Outline of Events:

1. Introduction and Setup

Scenario Briefing: Explain that the team will engage in a simulation involving a complex account creation request. The request appears to come from a senior leadership member via email such as APD Police Chief or one of his Deputy Chiefs.

Email Delivery: The team receives an email purportedly from the Chief's Office (generated by AI to mimic writing style) requesting the urgent creation of an account for a new external consultant who will be working closely with the department.

2. Initial Response

- Urgent Account Creation Request: The Helpdesk team receives an urgent directive, seemingly from the Chief's Office, to create a new user account for an external consultant. Due to the purported sensitivity and immediacy of the consultant's work, the email requests rapid handling of the account setup.
- Utilizing "Create Like" Functionality: To expedite the process, the Helpdesk staff member uses the "create like" functionality, which allows them to model the new account's permissions after an existing account, supposedly to ensure the consultant has all necessary access rights as directed in the request. This potentially over-permissions the account, increasing the risk of misuse. The Helpdesk employee is also not familiar with the "create like" account given – but does it anyway.
- First Plot Twist: The email only creates a Helpdesk ticket for the account creation request. The email may have come from an external source.`

3. Challenging Circumstances

- Limited Staffing: The request arrives during lunchtime, a peak low-staff period, leaving only one Helpdesk employee on duty to manage all incoming tasks.
- High Demand: The single staff member is already stretched thin, managing multiple walk-in requests and a steadily ringing phone queue with other support issues.

4. Impact of Pressure
   - Increased Risk of Error: The combination of high-pressure from a senior leadership request, use of expedited procedures, and the distractions from concurrent demands may lead to oversight and insufficient verification of the request's legitimacy.
   - Compromised Verification Process: Typically, thorough verification steps may be skipped or inadequately performed, such as directly confirming the request with the Chief's Admin or more carefully scrutinizing the email's authenticity.

5. Second Plot Twist: In their haste and under pressure, the Helpdesk staff member chooses to model the new account's permissions after a data consultant's account, known for having extensive admin-level access and VPN privileges. This action greatly amplifies the potential impact of any misuse of the account.

   Complication Due to Plot Twist:

   Immediate Consequences: The revelation that the fraudulent account now mirrors a high-level admin account with critical privileges goes unnoticed. The Helpdesk staff moves on to the next task in the queue. Nobody is aware of the potential that a malicious actor could now exploit these permissions to access confidential information or disrupt IT systems.

Enhanced Training Element Note:

Security Implications Discussion: This plot twist is intended to provide a teaching moment of the risks associated with 'create like' functionalities, especially under pressure. It underscores the necessity for stringent controls and checks when handling permissions, particularly for accounts that are rushed or requested under unusual circumstances.

Always remember: Malicious actors frequently succeed in achieving their objectives and carrying out their intended actions.

6. Third Plot Twist:

   The account creation request comes directly from cell phone text messaging or phone call/voicemail message.

PART TWO: Public Safety Department Compromise

Objective:

To enhance the preparedness and response capabilities of the Public Safety departments (Police, Fire, Community Service) in the event of a cybersecurity incident involving the compromise of their record-keeping systems.

Participants:

1. Police Department (APD)
2. Fire Department (AFR)
3. Community Service Responders (ACS)
4. Aviation (ABQ Sunport)
5. IT Security Team

Outline of Events:

1. Introduction and Setup

Scenario 1 Briefing: A department employee's credentials have been found on the dark web. Each department will be affected by a similar compromise in their record-keeping systems.

Scenario 2 Briefing: An account creation request, believed to be from a trusted source, is later deemed fraudulent and discovered to have over-permissioned access to your department's record systems. Each department will need to assess the impact of this fraudulent account on their reporting systems and databases.

2. Initial Response

Scenario 1: Department employee's credentials have been found on the Dark Web

The IT Security Team receives intelligence that CABQ credentials have been found on the dark web. The account's password is reset, and an investigation is launched.

Plot Twist 1: During the investigation, it is discovered that the compromised credentials were used to authorize a fraudulent account creation request, which had excessive permissions (ties into Scenario 2).

Discussion Points:

1. Methods for tracing the origin of the compromised credentials.
2. Reviewing application access logs for unusual or unauthorized activities.
3. Determine if any sensitive information was accessed or exfiltrated.

Connecting the Dots:

The IT Security Team identifies that the fraudulent account was created using the compromised employee's credentials, which appeared to be a legitimate request from within the organization.

Discussion Points:

1. The process by which the fraudulent account creation request was submitted and approved.
2. Identifying any lapses in the verification process for account creation.

Action Items:

1. Document the link between the compromised credentials and the fraudulent account creation.
2. Review and improve the account creation and verification process to prevent future incidents.

Plot Twist 2: Further analysis reveals that the fraudulent account had been used to create additional backdoor accounts and establish persistent access within the system.

Mitigation and Long-Term Solutions - Addressing the Broader Impact:

IT Security Team: Works on identifying and disabling all fraudulent and backdoor accounts created using compromised credentials.

Incident Response Team: Ensures all affected systems are secured and potential vulnerabilities are addressed.

Plot Twist 3: The investigation uncovers that similar fraudulent account creation attempts have been made using different employees' compromised credentials, indicating a broader targeted attack.

Discussion Points:

1. Steps to mitigate the broader impact of the compromised credentials.
2. Implementing long-term solutions to prevent similar incidents.

Action Items:

1. Document all actions taken to secure the systems.
2. Develop a long-term security improvement plan, including employee training and enhanced verification processes.

Scenario 2: Fraudulent Account Creation Request (such as BEC or AI-generated)

The IT Security Team receives reports of newly created accounts with suspiciously high levels of access across various departments. These accounts were created following a series of sophisticated phishing or AI-generated requests, believed to be from trusted sources within the organization.

1. Police Department: An account is created with full access to the incident management system (such as Mark/43).
2. Fire Department: An account is created with administrative access to the dispatch system (such as P1 CAD).
3. Community Service: An account is created with unrestricted access to client records (such as Caspio or Mark/43).
4. Aviation IT: An account is created with unrestricted access to airport IT systems.

Discussion Points:

1. How the suspicious accounts were detected.
2. Immediate actions to secure the systems and investigate the accounts.

Action Items:

1. Document initial detection methods.

2. Reset passwords and limit access for suspicious accounts.
3. Notify department heads and initiate a preliminary investigation.

Plot Twist 1: During the investigation, it is discovered that the account creation requests came through emails appearing to be from Director-level executives, using Business Email Compromise (BEC) tactics.

Tracing the Account Creation Requests:

The IT Security Team begins tracing the origin of the account creation requests to determine if they were part of a larger, coordinated attack.

Forensic Analysis is performed to review email logs, service requests and system access logs to identify patterns and potential sources of compromise.

Plot Twist 2: Forensic analysis reveals that the fraudulent account creation requests were facilitated by compromised credentials previously found on the dark web, linking back to the earlier account compromise scenario.

Mitigation and Coordination - Containing the Breach

Police Department: Revokes access and reviews system logs for any unauthorized activities by the fraudulent account.

Fire Department: Secures the (dispatch) system and verifies the integrity of the data.

Community Service: Conducts a full audit of client records to identify any data breaches.

Aviation IT: Implements emergency protocols to secure airport IT systems and reviews critical infrastructure for vulnerabilities.

Discussion Points:

1. Steps to mitigate the immediate threat and secure systems?
2. Coordination between departments and external agencies (e.g., FBI, cybersecurity firms)?

Action Items:

1. Document containment and mitigation steps.
2. Plan for coordinated response and communication with external agencies.

Plot Twist 3: It is discovered that the compromised credentials used for the fraudulent account creation were also used to create backdoor accounts, providing persistent access to the attackers.

Resolution and Recovery - Eradicating the Threat and Recovery

1. IT Security Team: Identifies and removes all AD backdoor accounts and ensures all systems are secured.
2. Incident Response Team: Conducts a thorough review of all systems (including local accounts) and implements enhanced monitoring.
3. Departments: Each department reviews and updates their access control policies to prevent future incidents.

Discussion Points:

1. Long-term solutions to prevent similar incidents.
2. Steps for recovering and restoring systems and data if data was manipulated.

Plot Twist 4: During the recovery phase, a new wave of phishing emails is detected, targeting employees with fake account creation requests, emphasizing the need for continuous vigilance and training.

Post-Incident Review and Lessons Learned

Debrief and Improvement

1. All Departments: Conduct a comprehensive review of the incident handling and response.
2. IT Security Team: Presents findings and recommendations for improving security measures and protocols.

Discussion Points:

1. Summary of the incident and response effectiveness.
2. Key lessons learned and areas for improvement.

Action Items:

1. Document these lessons learned.
2. Develop and implement recommended security measures.

3. Plan follow-up training and future tabletop exercises to test these new measures.

Provisions for Note Taking and Action Items

Note-Taking Templates:

- Provided templates for participants to document their actions, observations, and decisions.

Action Item Log:

- A shared action item log to track tasks assigned during the exercise and their completion status.

Feedback Forms:

- Post-exercise feedback forms to gather participant insights and suggestions for improvement.

Conclusion and Acknowledgments

Wrap-Up:

- Summarize the event's key takeaways.
- Thank participants for their engagement.
- Discuss next steps and any follow-up actions.

Templates

1. Sample Action Item Log

Sample Action Item Log Template

Action Item ID	Description of Action	Assigned To	Due Date	Status	Notes
AI-001					
AI-002					
AI-003					

2. Sample Feedback Form:

Sample Post-Exercise Feedback Form Template

Participant Name:

Role/Department:

1. What were the strengths of the exercise?

2. What were the weaknesses or areas for improvement?

3. Were the objectives of the exercise clear and achievable?

Yes / No (Circle one)

Comments:

4. How effective was communication and coordination between departments?

5. Were the scenarios realistic and relevant to your role?

Yes / No (Circle one)

Comments:

6. What key lessons did you learn from the exercise?

7. What additional resources or training would you recommend improving future exercises?

8. Any other comments or suggestions?

SCRIPT PART ONE: Operation Identity Check: Tabletop Exercise (2:00pm)

Introduction and Setup

Facilitator:

"Welcome, everyone, to our tabletop exercise, Operation Identity Check. Today, we will engage in a scenario designed to enhance the City's vigilance and proficiency in identifying and responding to fraudulent account creation requests. The scenario will involve advanced tactics like Business Email Compromise (BEC) and AI-generated fake identities, commonly known as DeepFakes.

This exercise will involve multiple Public Safety departments, including Police, Fire, and Community Service responders. Our goal is to test and improve our Helpdesk team's response capabilities under pressure. Let's begin with the scenario briefing."

~~~~~~~~~~~~~~

Scenario Briefing

Facilitator:

"Imagine it is a regular workday. Perhaps tomorrow is even a holiday. Our TSU Helpdesk team is functioning as usual, handling various support requests from our departments. Suddenly, an urgent email arrives, and it's from the Chief's Office. The email appears to be from a senior leadership member, such as the Police Chief or one of his Deputy Chiefs, and it requests the urgent creation of an account for a new external consultant who will be working closely with the department."

~~~~~~~~~~~~~~

Initial Response

Facilitator:

"The email instructs that the new account needs to be created immediately due to the sensitive nature of the consultant's work. To expedite the process, the TSU Helpdesk staff member performs the task directly in Active Directory and models the new

account's permissions after an existing account. This step is taken to ensure that the consultant has all necessary access rights as directed in the request."

Pause to let participants react and discuss.

~~~~~~~~~~~~~~

First Plot Twist

Facilitator:

"Now the TSU Helpdesk responds to an urgent request that has come in through the KACE ticketing system. However, upon closer inspection, it becomes apparent that the email may have originated from an external source, not from the Chief's Office – but this is initially unnoticed."

Pause for participant reactions and discussions on how to verify the legitimacy of the email.

~~~~~~~~~~~~~~

Challenging Circumstances

Facilitator:

"To complicate matters, this urgent request arrives during lunchtime, a peak low-staff period. Only one TSU Helpdesk employee is on duty, juggling multiple walk-in requests and a steadily ringing phone queue with other support issues."

Pause to allow participants to discuss strategies for managing high demand with limited staffing.

~~~~~~~~~~~~~~

Impact of Pressure

Facilitator:

"Under the pressure of a senior leadership request, and the high workload, the Helpdesk staff member may inadvertently skip any verification steps. This could include failing to directly confirm the request with the Chief's Admin or insufficiently scrutinizing the email's authenticity."
~~~~~~~~~~~~~~

Encourage participants to share their thoughts on maintaining verification processes under pressure.

~~~~~~~~~~~~~~

Second Plot Twist

Facilitator:

"In their rush and under pressure, the TSU Helpdesk staff member decides to model the new account's permissions after another data consultant's account, which has extensive admin-level access and VPN privileges. This action significantly increases the potential impact of any misuse of the account."

Allow time for participants to discuss the security implications of this decision and how to prevent similar mistakes.

~~~~~~~~~~~~~~

Immediate Consequences

Facilitator:

"The fraudulent account, now with high-level admin access, goes unnoticed. The TSU Helpdesk staff moves on to the next task, unaware of the potential for a malicious actor to exploit these permissions to access confidential information or disrupt IT systems."

Encourage discussion on the potential consequences and steps to mitigate such risks.

~~~~~~~~~~~~~~

Third Plot Twist

Facilitator:

"Now, instead, consider receiving an urgent account creation request - this time via cell phone text messaging or a phone call/voicemail message? What is done to validate the authenticity and details of the request?"

Pause for participants to discuss the challenges of verifying requests received through these channels.

~~~~~~~~~~~~~~

Enhanced Training Element

Facilitator:

"Let's take a moment to discuss the security implications of the 'create like' functionality, especially under pressure. This scenario highlights the necessity for stringent controls and checks when handling permissions, particularly for accounts requested under unusual circumstances. Also, what about verification techniques with Password Resets?"

Lead a discussion on best practices and lessons learned from the exercise. Ask the Helpdesk what other unusual circumstances they have experienced with account creation requests and document them.

~~~~~~~~~~~~~~

Conclusion

Facilitator:

"Thank you all for your participation and discussion. This exercise highlights the importance of maintaining rigorous verification processes, even under pressure, and the potential consequences of overlooking these steps. Let's apply these lessons and improve our response strategies. Great job, everyone."

End of exercise.
~~~~~~~~~~~~~~

SCRIPT PART TWO: Public Safety Department Compromise (3:30pm)

Introduction and Setup

Facilitator:

"Welcome back, everyone, to the second part of our tabletop exercise, Operation Identity Check. In this session, we will focus on enhancing the preparedness and response capabilities of our Public Safety departments in the event of a cybersecurity incident involving the compromise of each of their record-keeping systems. Our participants today include the Police Department, Fire Department, Community Service Responders, Aviation IT, and the IT Security Team.

~~~~~~~~~~~~~~

Scenario 1 Briefing: Employee Credentials Compromised

Facilitator:

"Scenario 1 involves the discovery of a department employee's credentials on the dark web. Each department will face a similar compromise in their record-keeping systems. The IT Security Team receives intelligence about the compromised credentials, and an investigation is launched.

During the investigation, it is revealed that the compromised credentials were used to authorize a fraudulent account creation request with excessive permissions. This links directly to Scenario 2. Let's explore the initial response to this situation."

~~~~~~~~~~~~~~

Initial Response to Scenario 1

Facilitator:

"The IT Security Team resets the compromised account's password and starts investigating. The investigation must focus on tracing the origin of the compromised credentials, reviewing application access logs for unauthorized activities, and determining if any sensitive information was accessed or exfiltrated."

Real life example: KCKS – PD files found for sale on dark web believed to be from Wichita KS (partner) breach.

Pause for participants to discuss tracing methods, log reviews, and data security checks

~~~~~~~~~~~~~~

First Plot Twist: Compromised Credentials Used for Fraudulent Account Creation

Facilitator:

"During the investigation, it is discovered that the compromised credentials were used to create a fraudulent account with excessive permissions. This account creation request appeared legitimate and was approved without proper verification."

Encourage participants to discuss the verification process for account creation and identify any lapses.

~~~~~~~~~~~~~~

Discussion Points and Action Items

Facilitator:

"Let's discuss how the fraudulent account creation request may have been submitted and approved. What would be the lapses in the verification process? Documenting these issues will help us improve our processes to prevent future incidents."

Participants discuss and document lapses and improvement suggestions.

~~~~~~~~~~~~~~

Second Plot Twist: Additional Backdoor Accounts Discovered

Facilitator:

"Further analysis reveals that the fraudulent account was used to create additional backdoor accounts, establishing persistent access within the system. The IT Security Team must now identify and disable all fraudulent accounts and backdoors."

Participants discuss steps to identify and disable fraudulent accounts.

~~~~~~~~~~~~~~

Mitigation and Long-Term Solutions

Facilitator:

"To address the broader impact, we need to ensure all affected systems are secured and potential vulnerabilities are addressed. This includes identifying similar fraudulent attempts using different employees' compromised credentials, indicating a broader targeted attack."

Participants discuss steps to mitigate broader impacts and develop long-term security plans.

~~~~~~~~~~~~~~

Scenario 2 Briefing: Fraudulent Account Creation Requests

Facilitator:

"In Scenario 2, we receive reports of newly created accounts with suspiciously high levels of access across various departments, following a series of sophisticated phishing or AI-generated requests."

~~~~~~~~~~~~~~

Initial Response to Scenario 2

Facilitator:

"Each department will assess the impact of these fraudulent accounts on their systems. The Police Department finds an account with full access to the records management system or data lake repository (such as P1, Mark/43 and Peregrine), the Fire Department discovers an account with administrative access to the dispatch system (such as P1, ProQA), Community Service (ACS) finds an account with unrestricted access to client records (such as Mark/43 and Caspio), and Aviation IT detects an account with unrestricted access to airport IT systems."

Pause for participants to discuss detection methods and immediate actions to secure systems.

~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

Plot Twist 1: BEC Tactics Uncovered

Facilitator:

"During the investigation, it was discovered that the account creation requests came through emails appearing to be from Director-level executives, using Business Email Compromise (BEC) tactics. The IT Security Team must trace the origin of these requests and perform forensic analysis. KACE Tickets may also be a factor in these requests."

Participants discuss tracing and forensic analysis techniques.

~~~~~~~~~~~~~~

Plot Twist 2: Link to Compromised Credentials

Facilitator:

"Forensic analysis reveals that these requests were facilitated by compromised credentials previously found on the dark web, linking back to the earlier account compromise scenario."

Participants discuss how to secure systems and mitigate the immediate threat.

~~~~~~~~~~~~~~

Mitigation and Coordination

Facilitator:

"Each department must now revoke access, review application/system logs, and ensure the integrity of their data. Coordination between departments and external agencies, such as the FBI or cybersecurity firms, is crucial. Additionally, it's important to consider the threshold for reporting the incident to third-party agencies, such as the State's Department of Public Safety (DPS) or the CABQ Public Information Officer. This decision involves evaluating the scope and impact of the incident to determine if external reporting is necessary."

Steps to Consider: Revoke Access, Log Review, Data Integrity, Coordination with External Agencies…

> Revoke Access: Immediately revoke access for the fraudulent accounts to prevent further unauthorized activities.

Log Review: Conduct a thorough review of application and system logs to identify any unusual or unauthorized activities.

Data Integrity: Ensure the integrity of your department's data by verifying that no sensitive information has been accessed or altered.

Coordination with External Agencies:

Evaluate the incident's impact and determine if it meets the threshold for reporting to third-party agencies.

If the threshold is met, prepare a detailed report for submission to DPS or the CABQ Public Information Officer.

Coordinate to ensure a unified and effective response to the incident.

Internal Reporting: Inform department heads and key stakeholders about the incident and the steps being taken to mitigate it.

Preliminary Investigation: Initiate a preliminary investigation to gather all necessary information and evidence related to the incident.

Also, what would OEM's process look like?

Participants discuss steps for revocation, log review, and inter-departmental coordination and the process for determining the threshold for reporting to third-party agencies.

~~~~~~~~~~~~~~

Plot Twist 3: Discovery of Backdoor Accounts

Facilitator:

"The investigation uncovers that the compromised credentials were used to create backdoor accounts, providing persistent access to the attackers. The IT Security Team must identify and remove all backdoor accounts."

Participants discuss the identification and removal of backdoor accounts.

~~~~~~~~~~~~~~

Resolution and Recovery

Facilitator:

"The IT Security Team conducts a thorough review of all systems and implements enhanced monitoring. Each department reviews and updates their access control policies. What does this look like? "

Participants discuss long-term solutions and recovery steps.

~~~~~~~~~~~~~~

Plot Twist 4: New Phishing Wave Detected

Facilitator:

"During the recovery phase, a new wave of phishing emails is detected, targeting employees with fake account creation requests. This emphasizes the need for continuous vigilance and training."

Participants should discuss continuous vigilance and training strategies.

~~~~~~~~~~~~~~

Post-Incident Review and Lessons Learned

Facilitator:

"To conclude, we will conduct a comprehensive review of the incident handling and response. The IT Security Team will present findings and recommendations for improving security measures and protocols."

Participants discuss the incident summary, effectiveness of the response, and key lessons learned.

Facilitator:

"Thank you all for your participation and insights. This exercise has highlighted the importance of stringent verification processes, inter-departmental coordination, and continuous vigilance. Let's document these lessons and develop a plan for follow-up training and future tabletop exercises. Great job, everyone."

End of exercise.

Session #1 Notes:

1. Some DTI Employees are not confident in the event that something goes wrong, they will know what to do/who to contact if their usual escalation contacts are not in the office/out of town.
2. Most of the DTI Employees knew about voice recognition/voiceover scams, however some were naïve/not familiar with this scam. Also, some people were not aware of "click here" scams via our Internal Outlook Inboxes.
3. DTI Employees know the basics about verifying who the caller is, etc. However, they were not so knowledgeable about how to tell if the person on the other line was really the contact that called them/they contacted.
4. The DTI Employees who participated seem to have the best interest of COA/the Constituents and want to do the right thing for everyone involved. They seem to be innovative about how we can tackle these scams and protect everyone all around us.

Session #2 Notes:

1. Identity check preparedness in event of cyber security incident.
2. Security would perform log checks, check trend, azure for suspicious logins
3. Mark 43 can check for accounts created and which access was given
4. Records reaches out to the Helpdesk for account creation or removal of access.
5. What monitoring is put in place to avoid back door creation? - reports are manual review.
6. Aviation can isolate itself from downtown traffic if need be.
7. Position changes are problematic due to non-removal of previous access roles.
8. Needs to be some type of stewardship and a review of accounts.
9. Better communication with HR to have the correct information in PeopleSoft. That way it can flow down to AD.

Session #2 Participant Comments:

[Mark/43] “Every user account can only pull datasets of 5,000 rows at a time if permissions are gained to access the analytics module which also limits each user to 10 queries per hour. A malicious person can do more damage deleting police reports than a productive data miner within that application.”