**Module 6 Project: Incident Response Risk Management and Cloud Essentials**

**Executive Summary**

SecureCart Inc., a hybrid e-commerce company, recently identified critical vulnerabilities in its Identity and Access Management (IAM) configurations and lacked a formal Incident Response Plan (IRP), leaving the organization exposed to insider threats, phishing attacks, and unauthorized access. A comprehensive security overhaul was initiated to address these gaps and enhance the company's overall cybersecurity posture.

Key issues discovered in the IAM structure included excessive privilege assignments, improper group memberships, and unrestricted guest access. Notably, an IT Analyst was granted Global Administrator rights, an IT Manager was incorrectly assigned to the Finance group, and marketing contractors had unrestricted access to internal SharePoint resources. These misconfigurations posed a significant risk to operational integrity and data confidentiality.

To resolve these issues, the project implemented the principle of least privilege and Role-Based Access Control (RBAC) using Microsoft Entra ID. Administrative roles were reassigned appropriately, structured security groups were created for departments lacking them, and guest access was restricted to only necessary marketing resources. Conditional Access Policies were also introduced to enforce Multi-Factor Authentication (MFA), block high-risk sign-ins, require password resets for medium-risk users, and limit access based on geographic location.

In parallel, a phishing simulation was conducted using Microsoft Defender's Attack Simulation Training. This simulation mimicked a credential harvesting attempt, allowing the security team to walk through the full NIST 800-61 IRP lifecycle—from preparation to post-incident review. Entra ID sign-in logs and Defender dashboards were used to analyze behavior, detect anomalies, and take containment and recovery actions.

As a result of these interventions, SecureCart Inc. significantly strengthened its cloud security posture. The company now operates with cleaner access structures, stronger authentication controls, and a tested response plan that prepares it to quickly and effectively respond to future incidents.

**2. Identity and Access Management (IAM) Implementation Report**

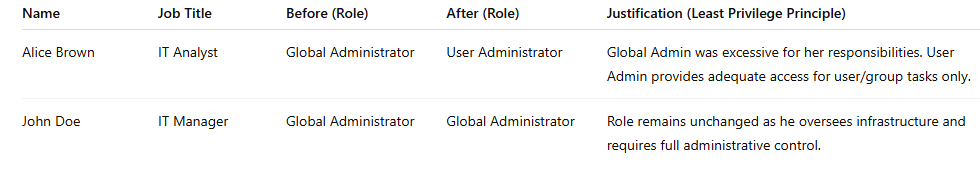
**2.1 Correct Role Assignments for IT Department**

During the IAM audit, it was discovered that administrative roles were not properly aligned with staff responsibilities in the IT department. Specifically:

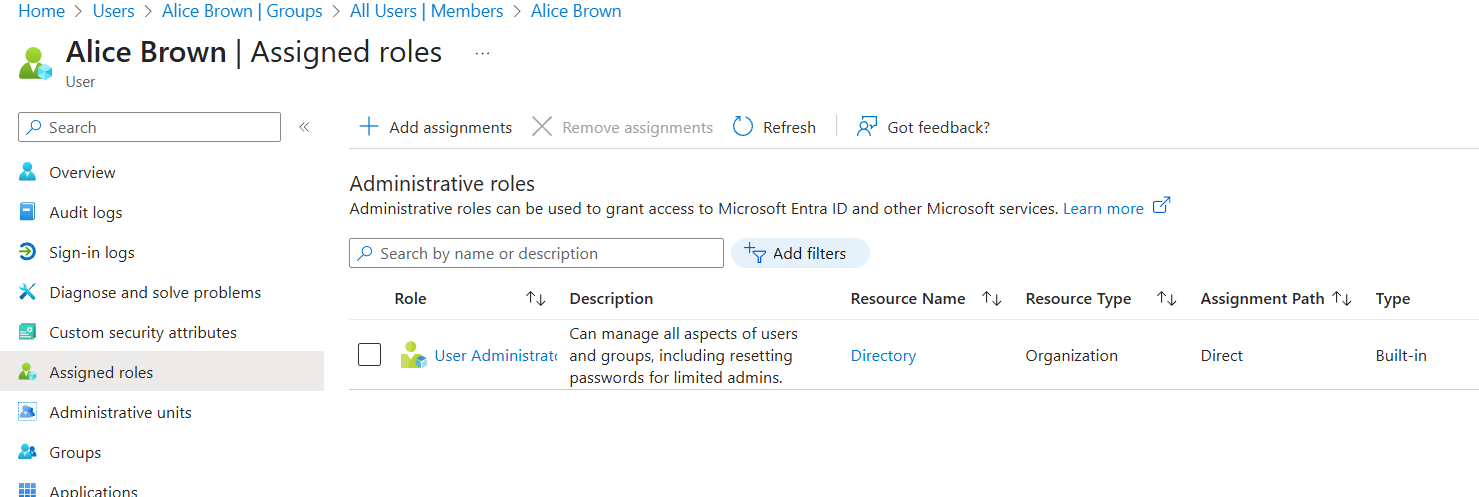
Alice Brown, an IT Analyst, had been granted Global Administrator privileges — a level of access beyond her operational duties and in violation of the least privilege principle.

John Doe, the IT Manager, was correctly assigned the Global Administrator role and required no changes.

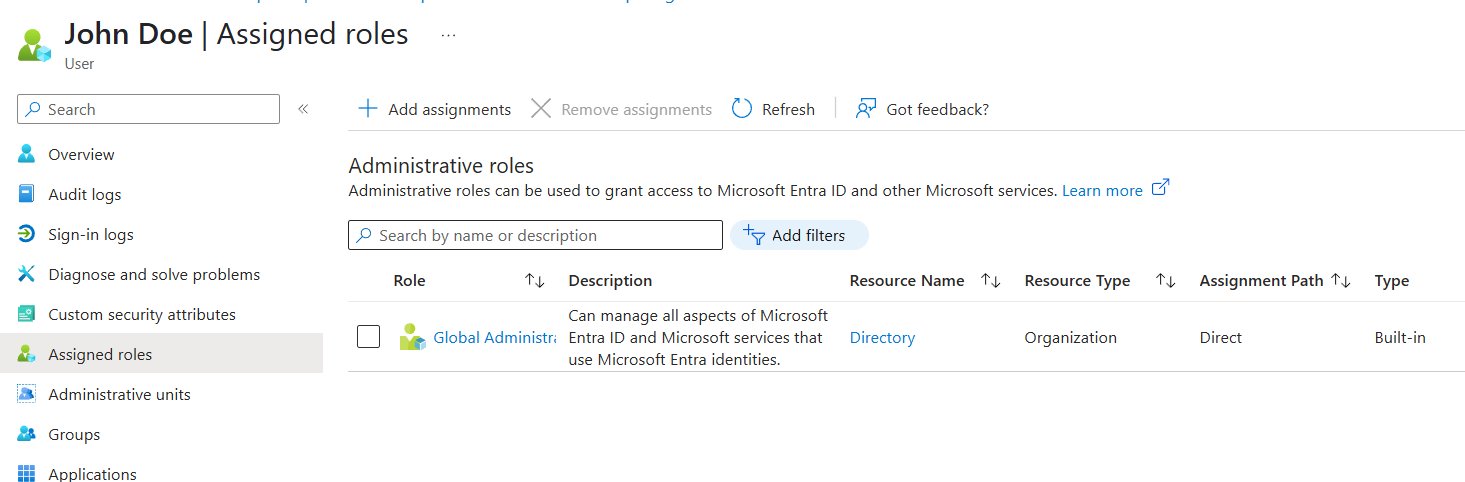
To correct this misconfiguration, role assignments were updated to ensure that users only had the minimum permissions necessary for their job functions.



**Screenshot: Assigned role for Alice Brown:**



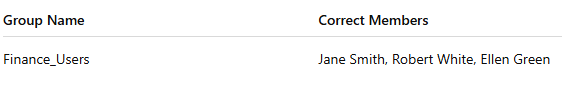
**Screenshot: Assigned role for John Doe:**



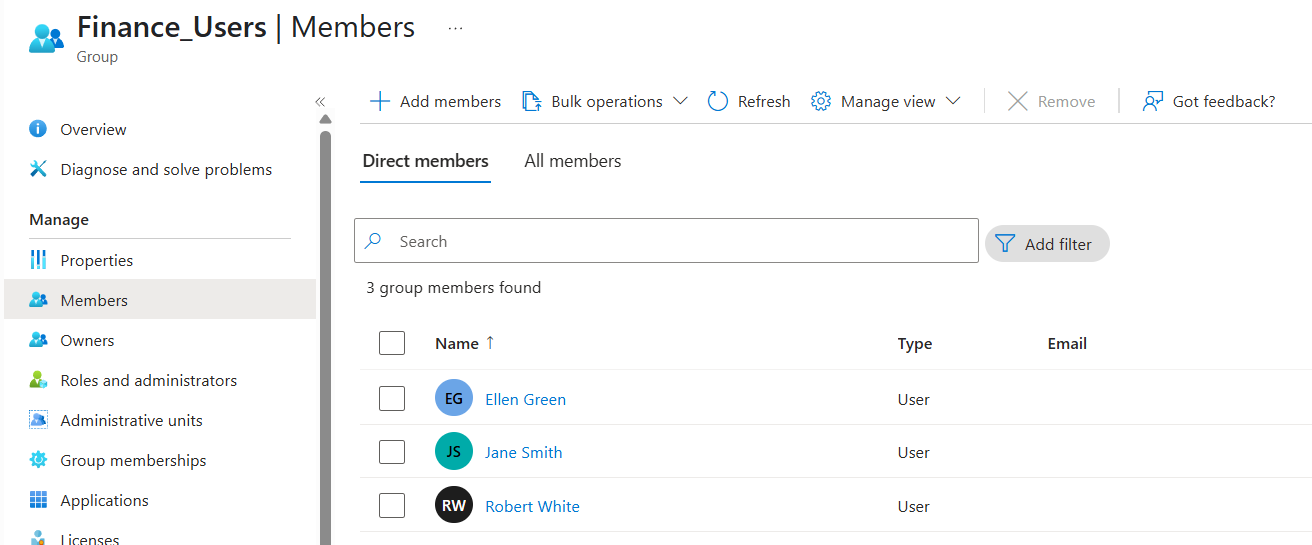
**2.2**

After reviewing the Finance\_Users group, it was discovered that John Doe, who is an IT Manager, was incorrectly assigned to the group. He had unnecessary access to sensitive financial applications like Microsoft Dynamics 365.

The group membership was corrected to include only legitimate Finance staff:



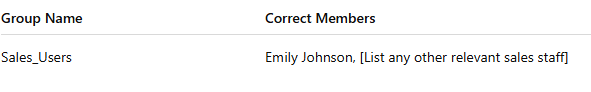
**Screenshots of updated Finance\_Users group membership.**

****

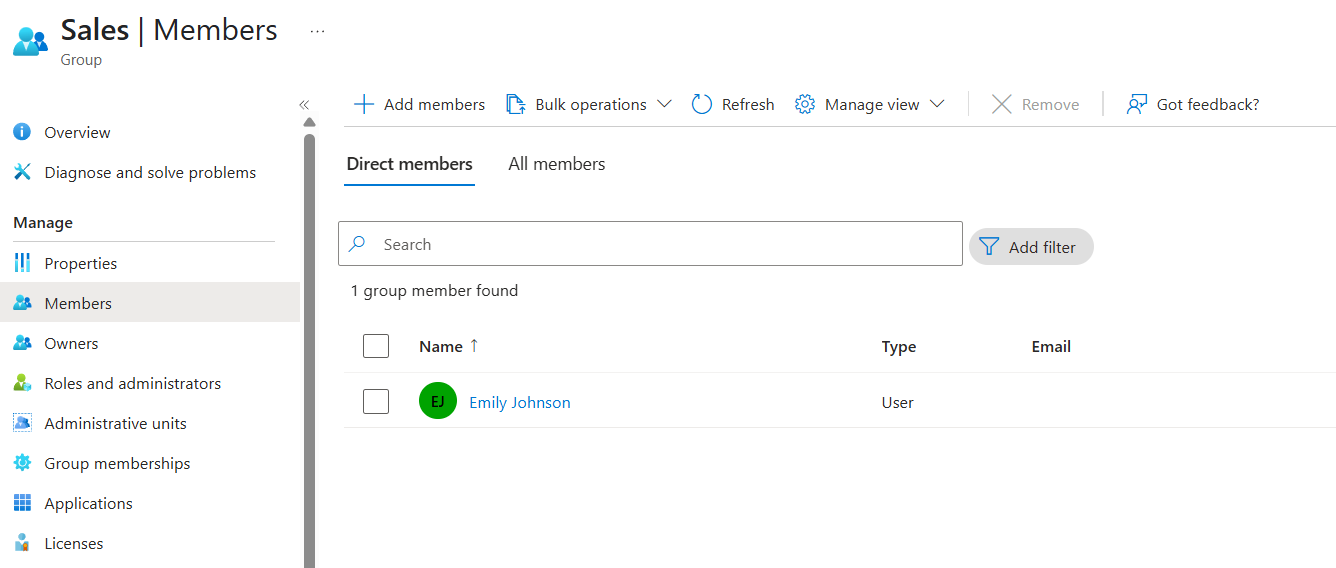
**2.3**

During the IAM audit, it was discovered that Emily Johnson, the Sales Manager, was not assigned to the Sales\_Users group, which prevented her from accessing the CRM tools required for managing customer accounts and processing orders.

This was corrected by adding her to the Sales\_Users group along with other authorized sales team members.



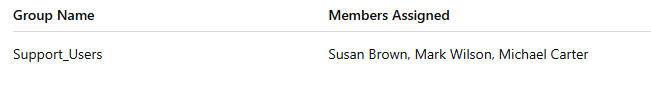
**Screenshots of group membership verification.**



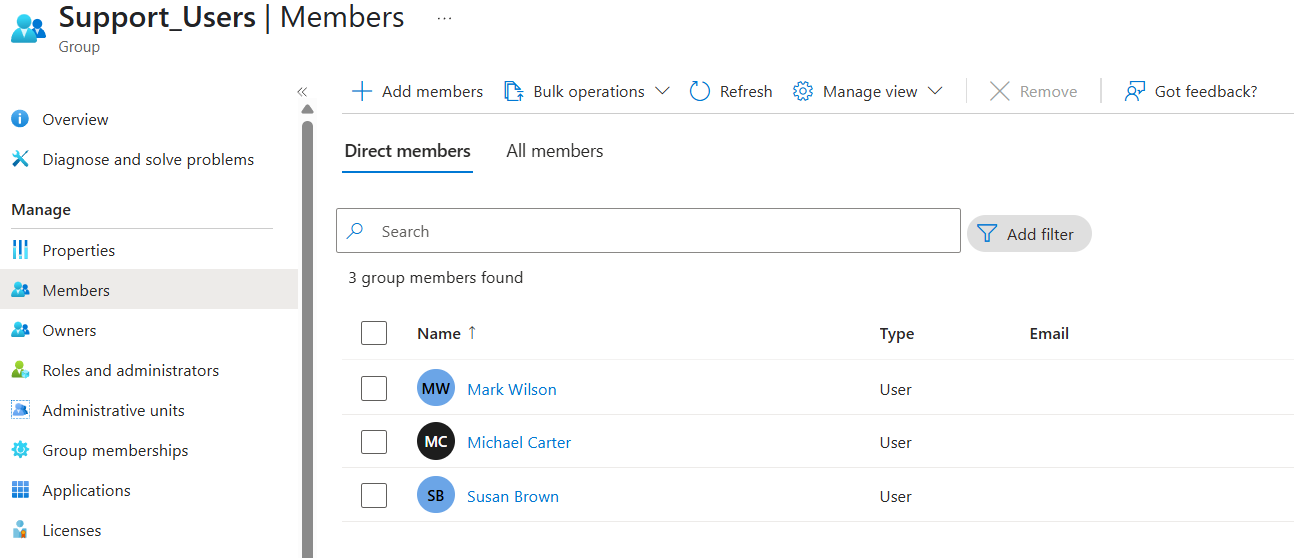
**2.4**

During the IAM review, it was discovered that the Customer Support Department lacked a structured security group, leading to inconsistent access control across support tools such as Freshdesk and internal user profiles.

To address this, a new group named Support\_Users was created in Microsoft Entra ID to centralize access management for all support agents.



**Screenshots of assigned users (Susan Brown, Mark Wilson, Michael Carter).**

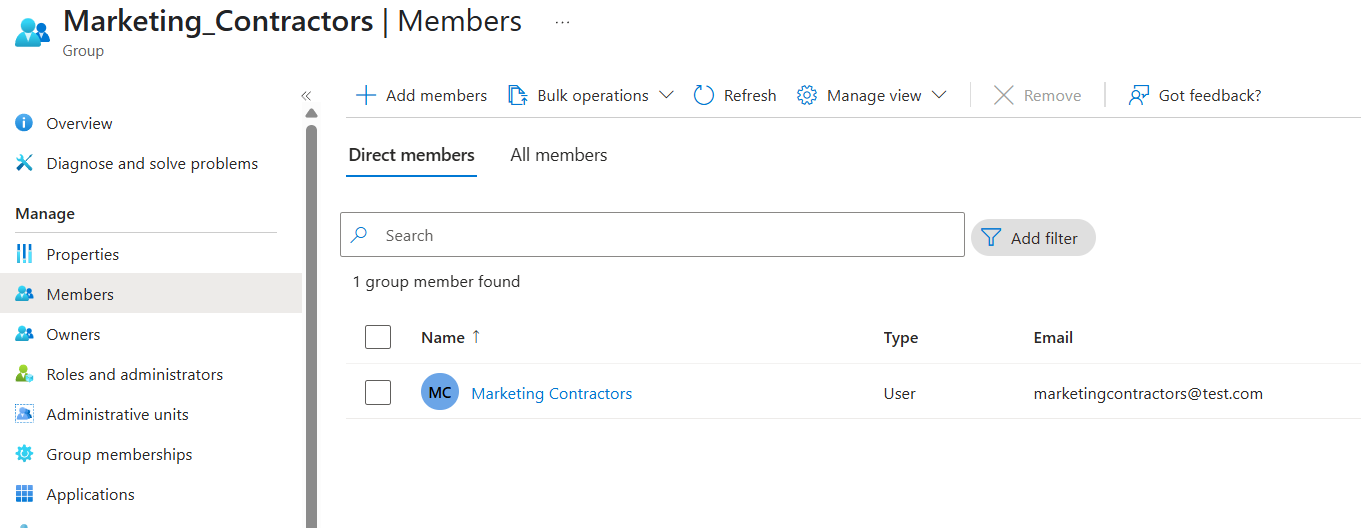


**2.5**

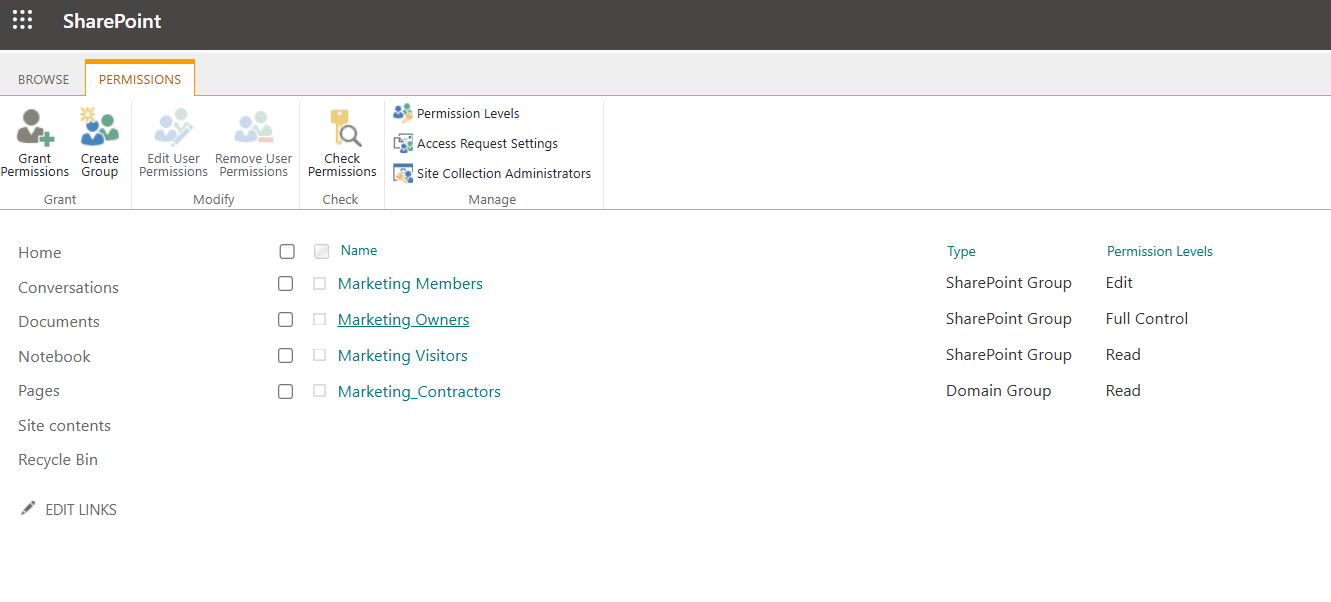
During the IAM audit, it was found that guest users supporting the Marketing Department had unrestricted access to all SharePoint folders and Microsoft Teams channels. This posed a significant data exposure risk, as external contractors could potentially view confidential or unrelated internal content.

To address this issue, a new security group named Marketing\_Contractors was created in Microsoft Entra ID to manage and limit guest access. Access controls were then refined in SharePoint Online and Microsoft Teams to ensure guests only have visibility into marketing-specific resources.

**Screenshot of Assigned User:**



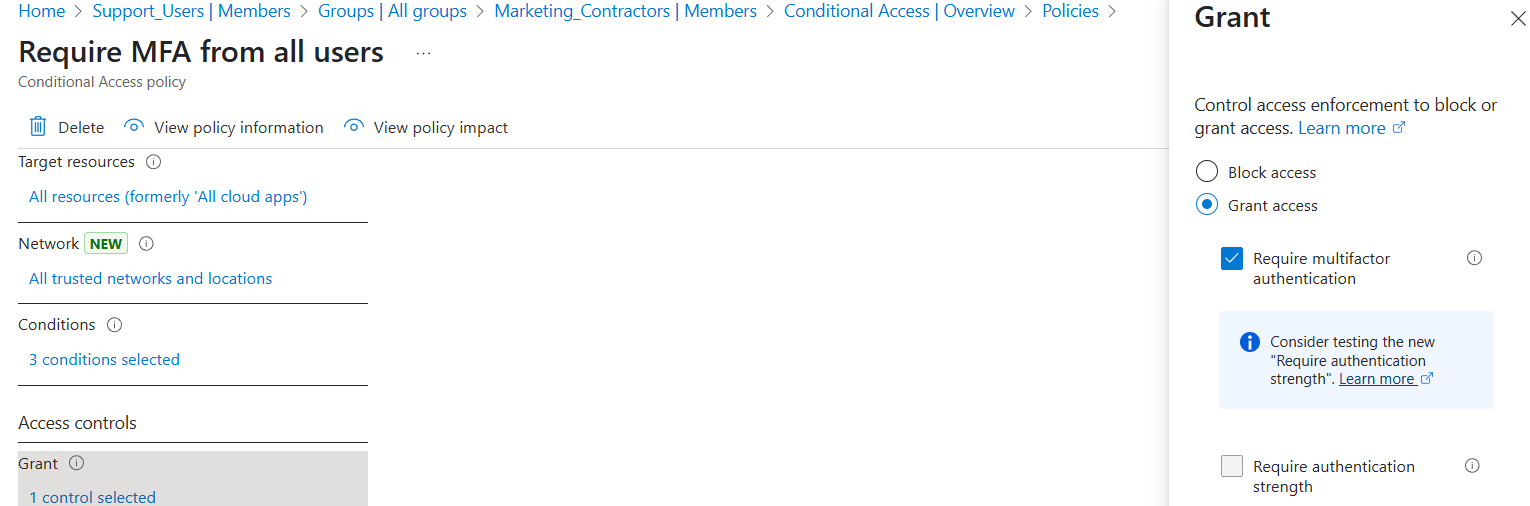
**Screenshots of applied restrictions in SharePoint Online and Microsoft Teams.**

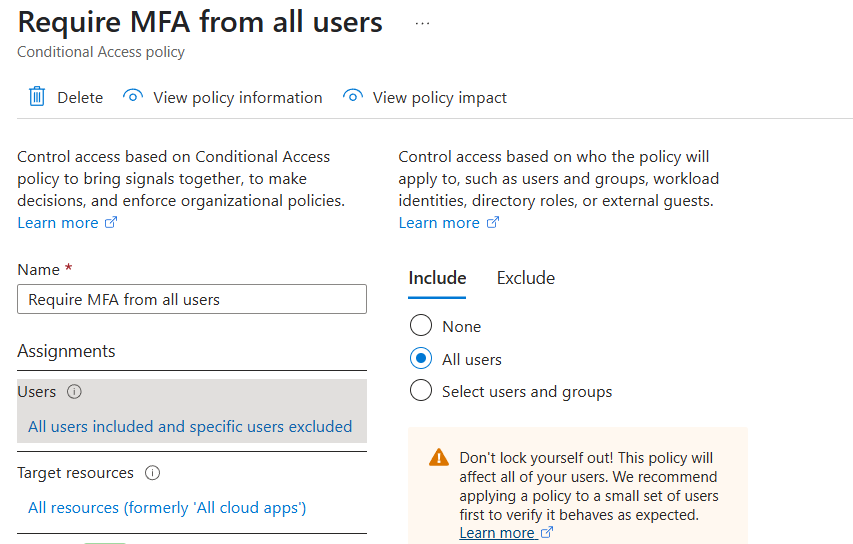


**3. Conditional Access Policies Report**

**3.1 Enforce Multi-Factor Authentication (MFA)**

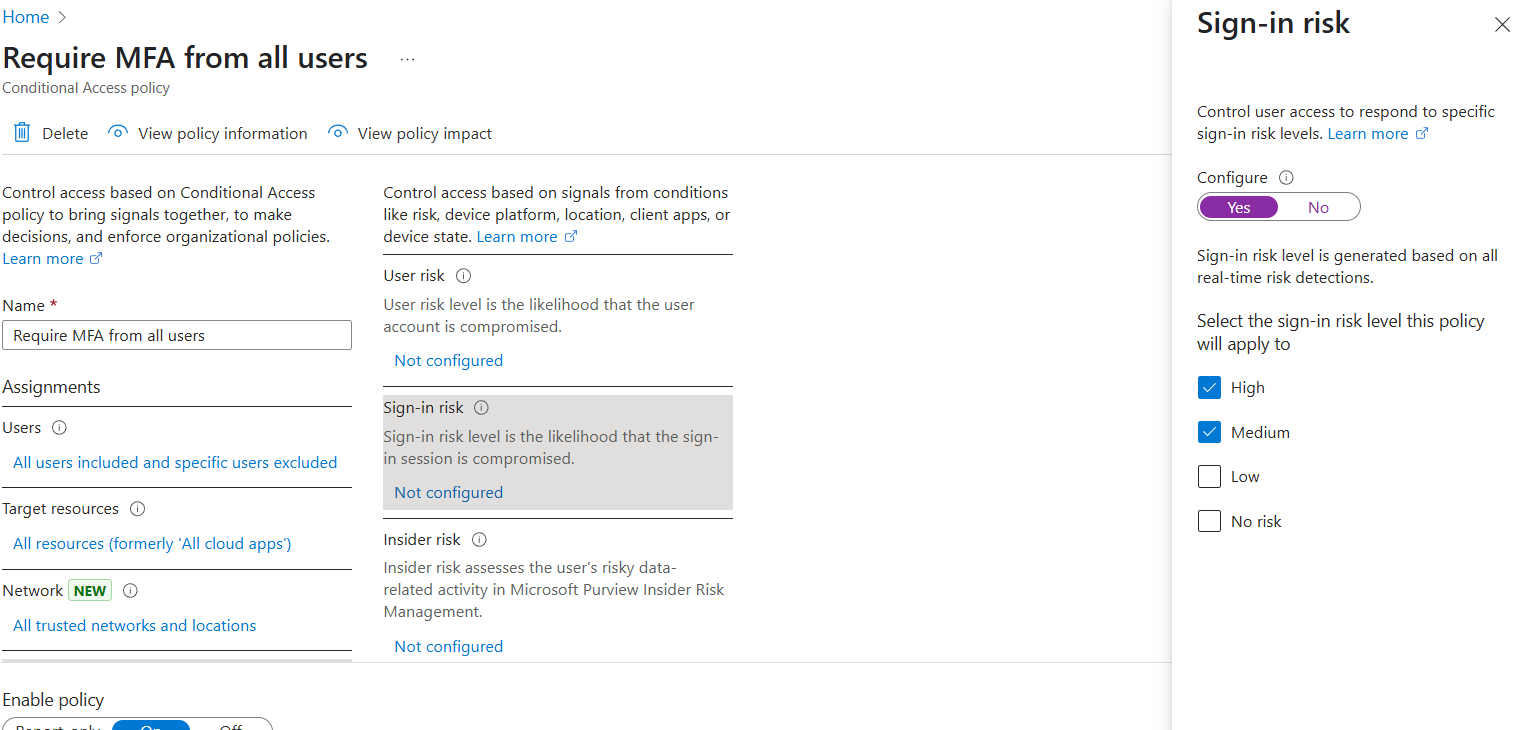
Enforcing MFA for all users reduces the risk of account compromise due to weak or stolen passwords. This policy ensures that even if credentials are phished, unauthorized access attempts will be blocked without a second verification step.

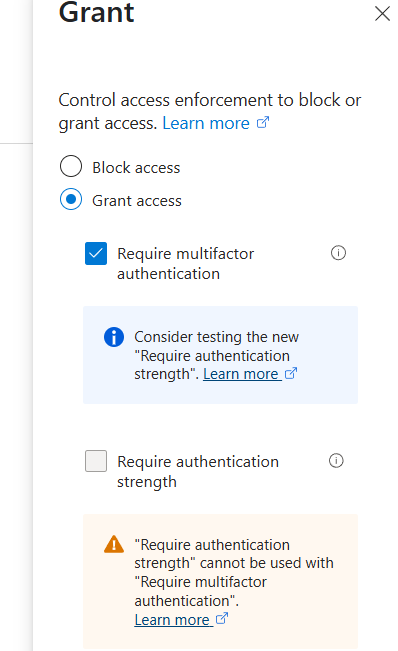
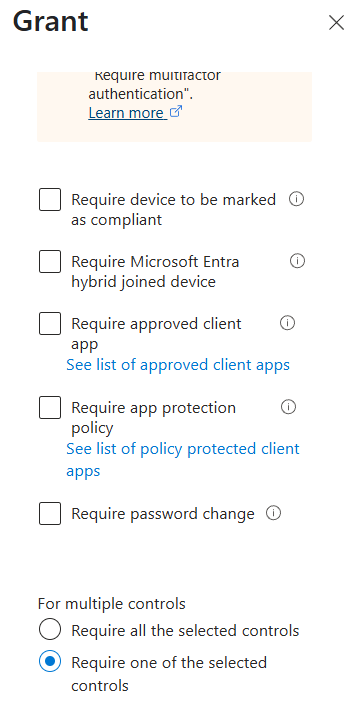
****

****

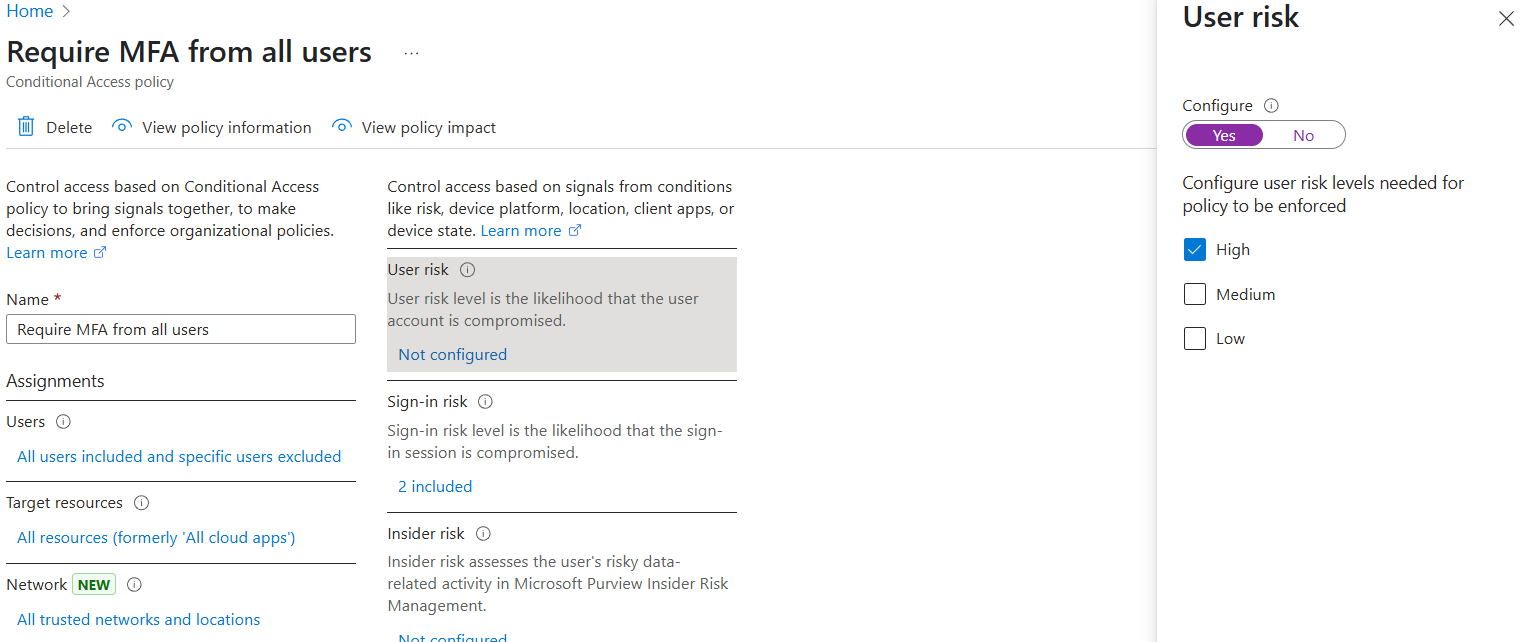
**3.2 Configure Sign-In Risk Policy**

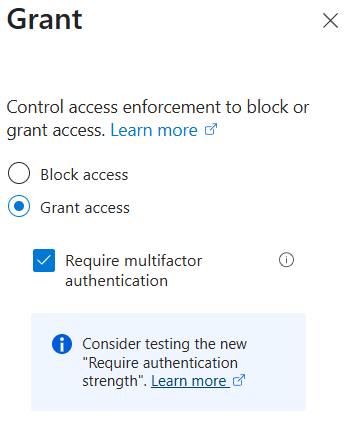
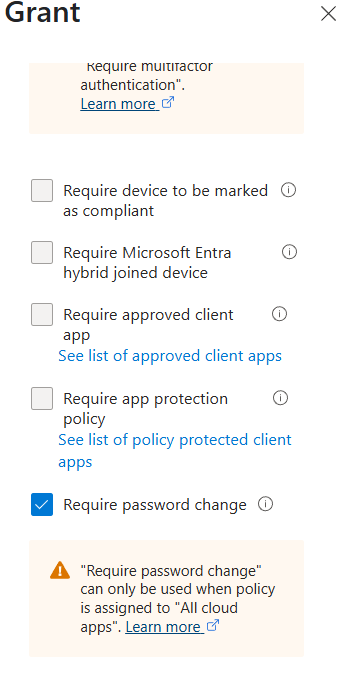
Screenshots of policy settings in Microsoft Entra ID.



**3.3 Configure User Risk Policy**



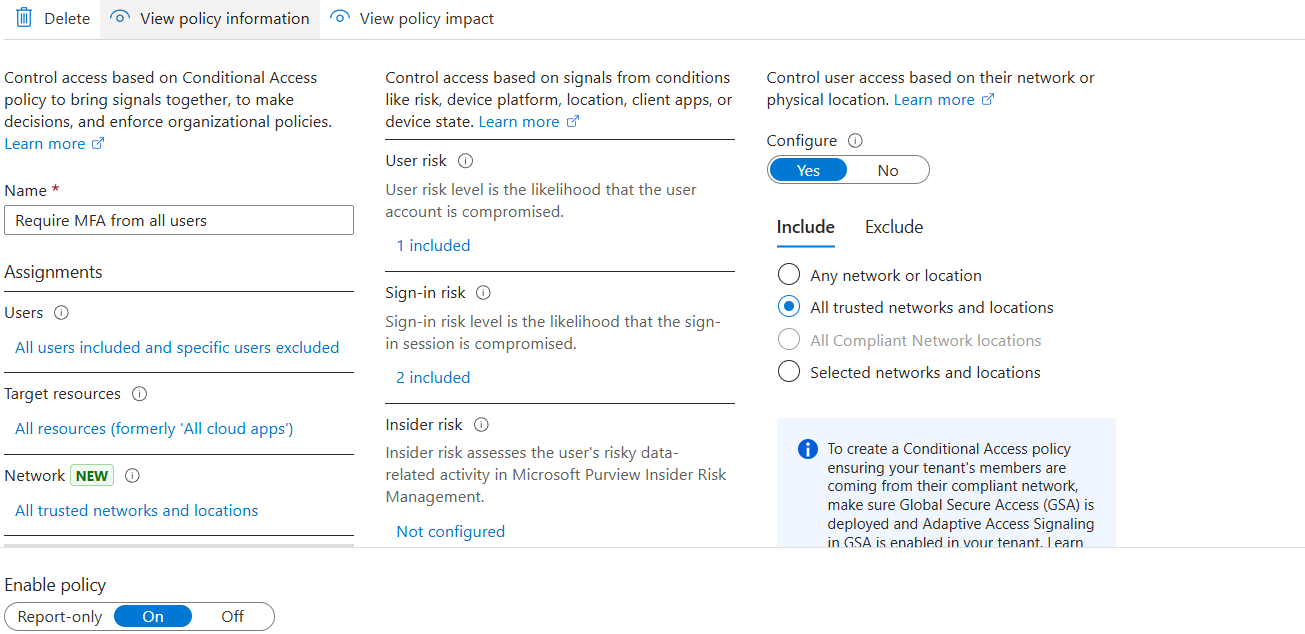
 

**3.4 Implement Location-Based Conditional Access.**

While setting up the location-based Conditional Access policy, I initially intended to restrict access to specific countries like the United States and Canada. However, the option to select individual countries didn’t appear during configuration.

As an alternative, I chose to apply the “All trusted networks and locations” option available in Microsoft Entra. This setting uses Microsoft’s built-in trusted IP ranges — such as those associated with Office 365 services and any preconfigured corporate IPs — to define what’s considered a safe location.

**Screenshots of configured geographic restrictions and policy enforcement logs:**



**4.1 NIST 800-61 Incident Response Plan**

This Incident Response Plan (IRP) follows the NIST 800-61 framework and is based on a phishing simulation that targeted Oluwaseun Akinola, a user within SecureCart Inc. The simulation aimed to test the organization's readiness to detect, contain, and recover from a cloud-based phishing attack using tools available in Microsoft 365 Defender and Microsoft Entra ID.

**1. Preparation**

To prepare for incidents, SecureCart Inc. established a dedicated Incident Response Team (IRT) with clearly defined roles:

Incident Response Coordinator – Manages the process (Oluwaseun Akinola in a training role)

Security Analyst – Reviews Defender alerts and Entra logs

System Administrator – Performs account-level and access-related changes

Communications Officer – Alerts stakeholders and users of ongoing threats

**Pre-incident measures included:**

Enforcement of Multi-Factor Authentication (MFA)

Conditional Access policies for location and sign-in risk

Security awareness training and periodic phishing simulations

**Tools used:**

Microsoft 365 Defender Portal

Entra ID Sign-in Logs

Conditional Access dashboards

Audit logs

**2. Detection & Analysis**

In the phishing simulation, Oluwaseun Akinola received an email impersonating an internal request for urgent payment processing. He clicked the embedded link and submitted credentials, simulating a successful account compromise.

Indicators and detection methods:

Defender Attack Simulation results flagged Oluwaseun’s interaction as a compromise

Entra ID sign-in logs captured the login event and IP activity

Defender marked the incident with risk indicators for analysis

**3. Containment**

Upon detecting the compromised credentials, immediate containment actions were taken:

The phishing email was quarantined in Defender

Oluwaseun’s account was temporarily disabled to prevent unauthorized access

Conditional Access settings were used to block the attacker’s IP (based on Entra log data)

These actions minimized potential escalation and stopped further credential abuse.

**4. Eradication**

After isolating the threat:

All active sessions for Oluwaseun’s account were revoked

A password reset was forced before re-enabling access

A full mailbox scan was conducted to ensure no malicious rules or hidden payloads were present

**5. Recovery**

Following eradication:

Oluwaseun’s account was reactivated with a secure, updated password

Access was closely monitored for unusual activity

Audit logs were reviewed to ensure no additional compromise occurred

Conditional Access policies remained in effect for future sign-ins

**6. Post-Incident Activities**

To wrap up the incident response process:

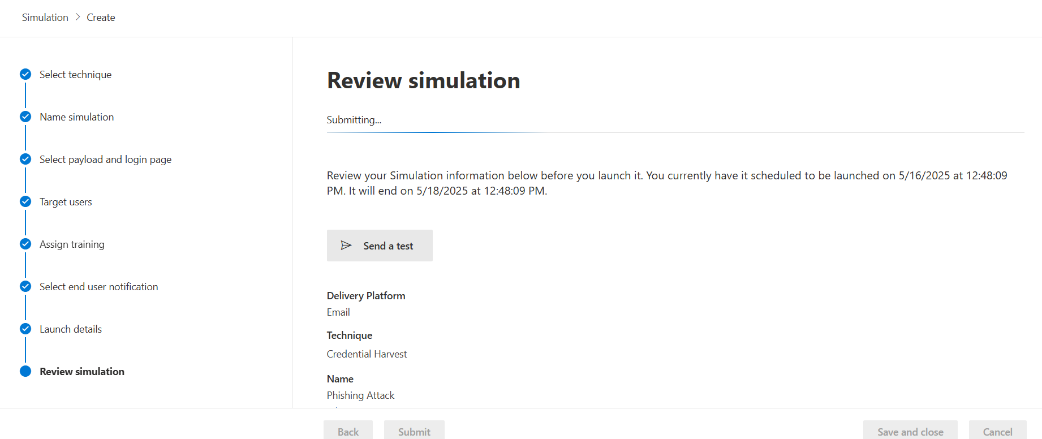
A lessons learned session was conducted

The IRP was updated to reflect real-world simulation outcomes

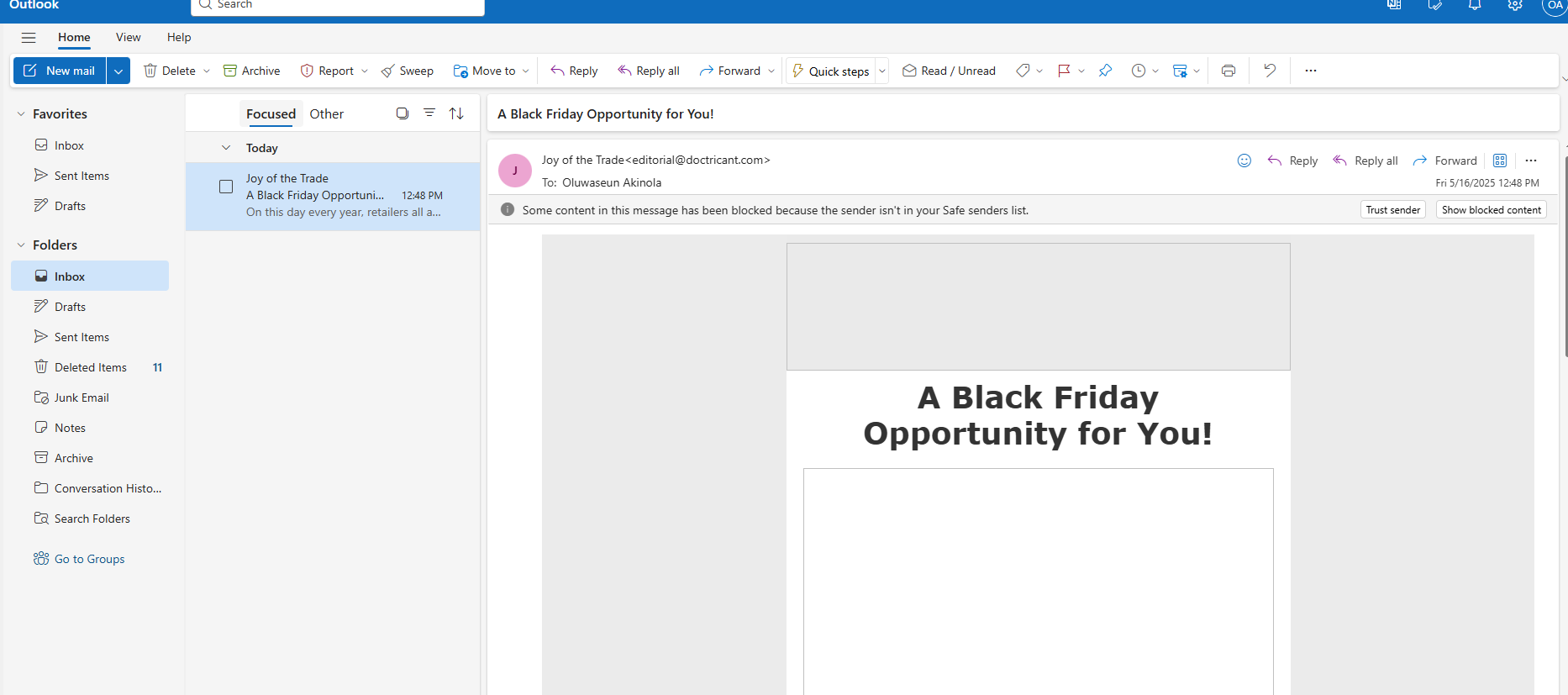
The phishing simulation data was used to reinforce training efforts

Additional phishing scenarios were scheduled to keep users vigilant

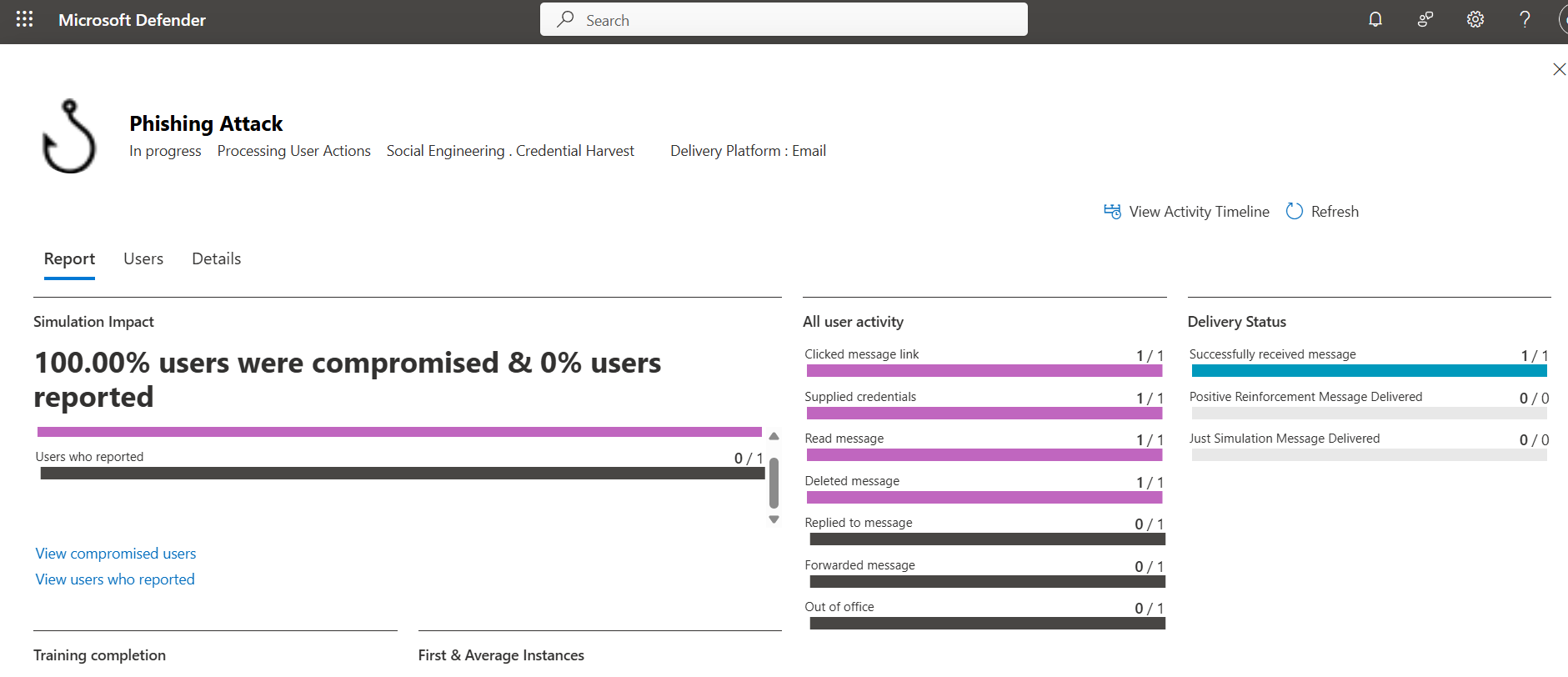
**5. Phishing Simulation Analysis & Documentation**

**5.1 Microsoft Defender Attack Simulation Results**

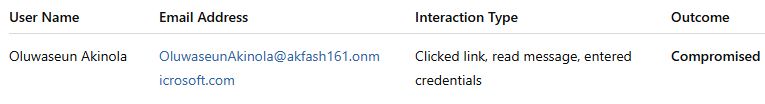
**Phishing Email:**



**Screenshots from the Attack Simulation Dashboard displaying test results:**



**List of Users Who Interacted with the Phishing Email:**

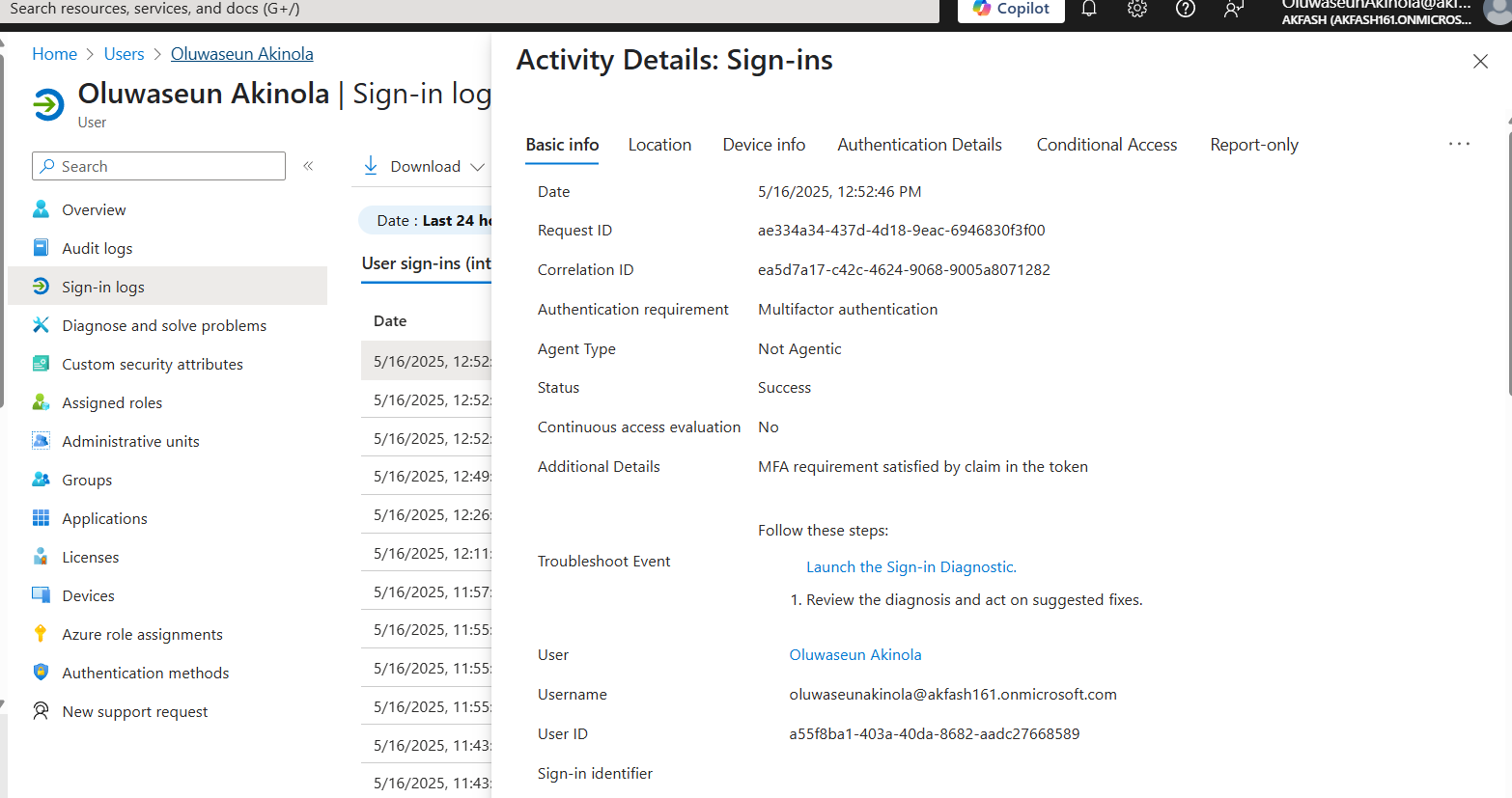


**5.2 Entra ID Log Analysis for Phishing Attempt**

The log confirms that the user successfully authenticated using MFA during the simulated phishing attack. While the authentication was technically valid, it was triggered by a simulated credential submission, mimicking a real-world compromise. This reinforces the importance of conditional access policies and behavior-based risk evaluation to detect potentially malicious sign-ins, even when credentials and MFA are correctly used.

This entry illustrates how attackers can bypass traditional defenses like MFA when users are socially engineered into willingly supplying credentials.

**Screenshots of audit logs capturing unauthorized access attempts:**



**5.3 Incident Documentation & Reporting**

**1. How the Phishing Attempt Was Detected**

**2. How the compromised account was contained and recovered.**

**3. Evidence supporting investigation findings (logs, screenshots).**

The phishing simulation was initiated using Microsoft Defender Attack Simulation Training, where a crafted phishing email titled "A Black Friday Opportunity for You!" was delivered to Oluwaseun Akinola’s inbox. The message appeared to be from "Joy of the Trade"

(editorial@doctricant.com) and mimicked a promotional offer to trick the user into clicking a malicious link.

Microsoft Defender's dashboard recorded that the user:

Opened the email

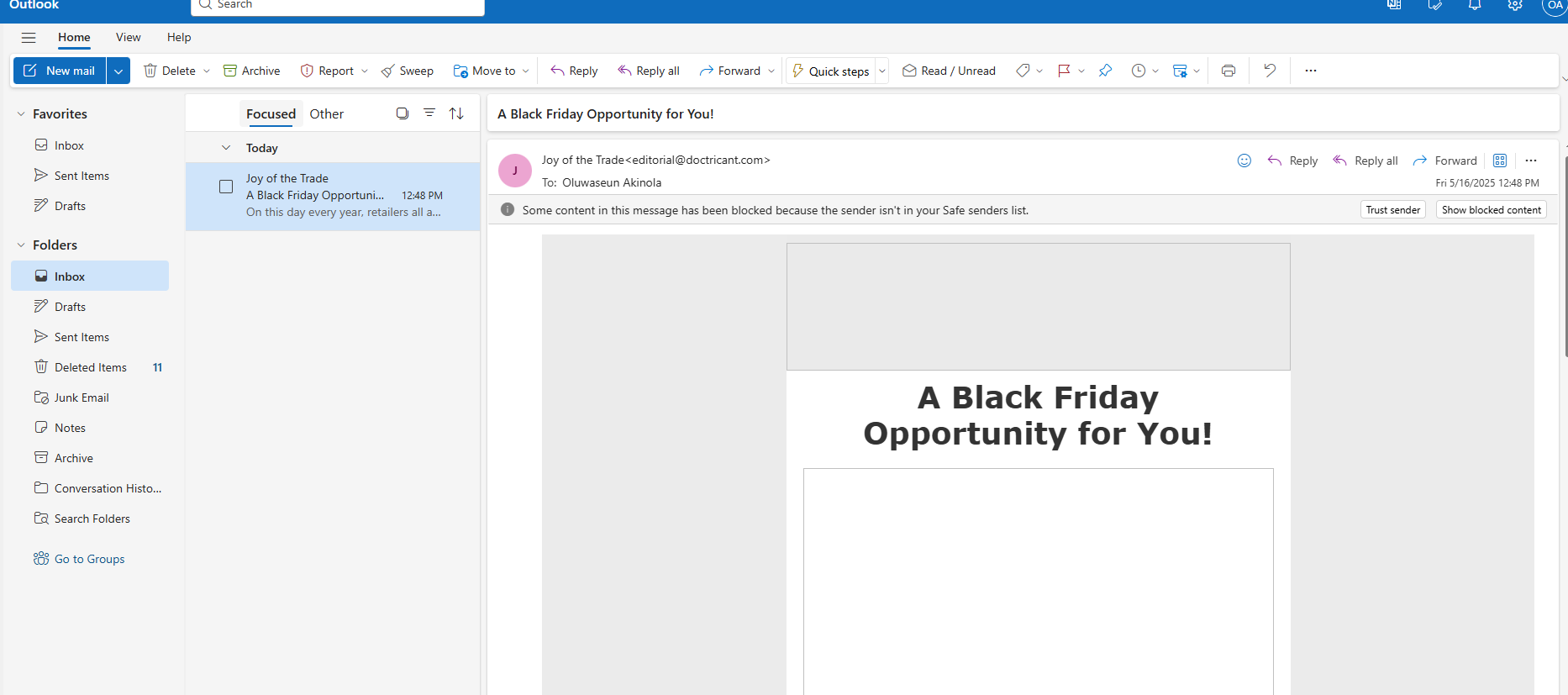
Clicked the message link

Supplied credentials on the phishing landing page

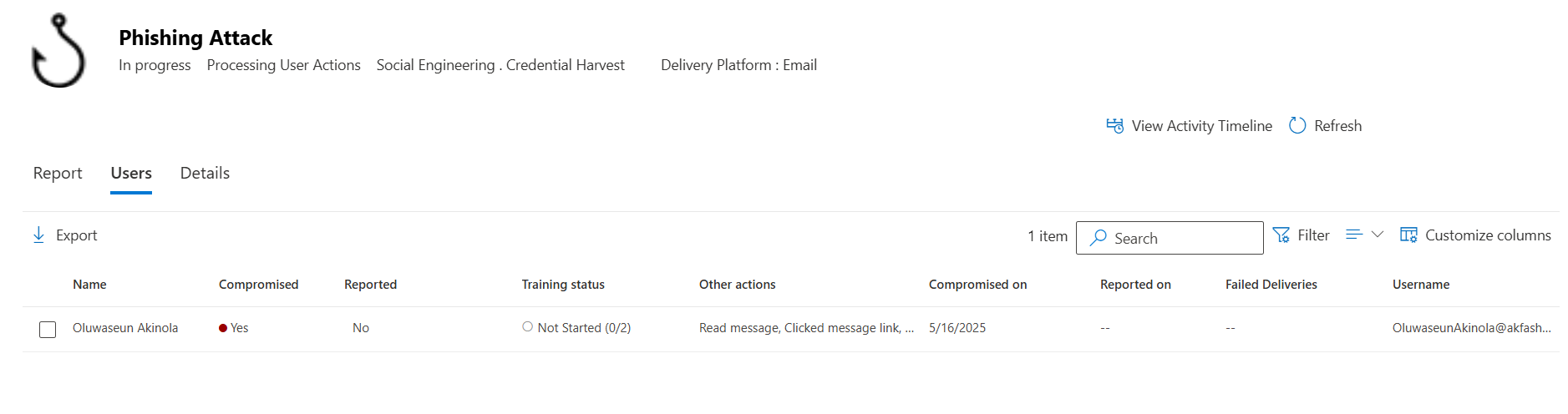
This activity was immediately visible in the Attack Simulation Report, confirming that 100% of targeted users were compromised, and 0% reported the message. The simulation also redirected the user to a training page, which explicitly stated:

"Oluwaseun Akinola, you were just phished by your security team."

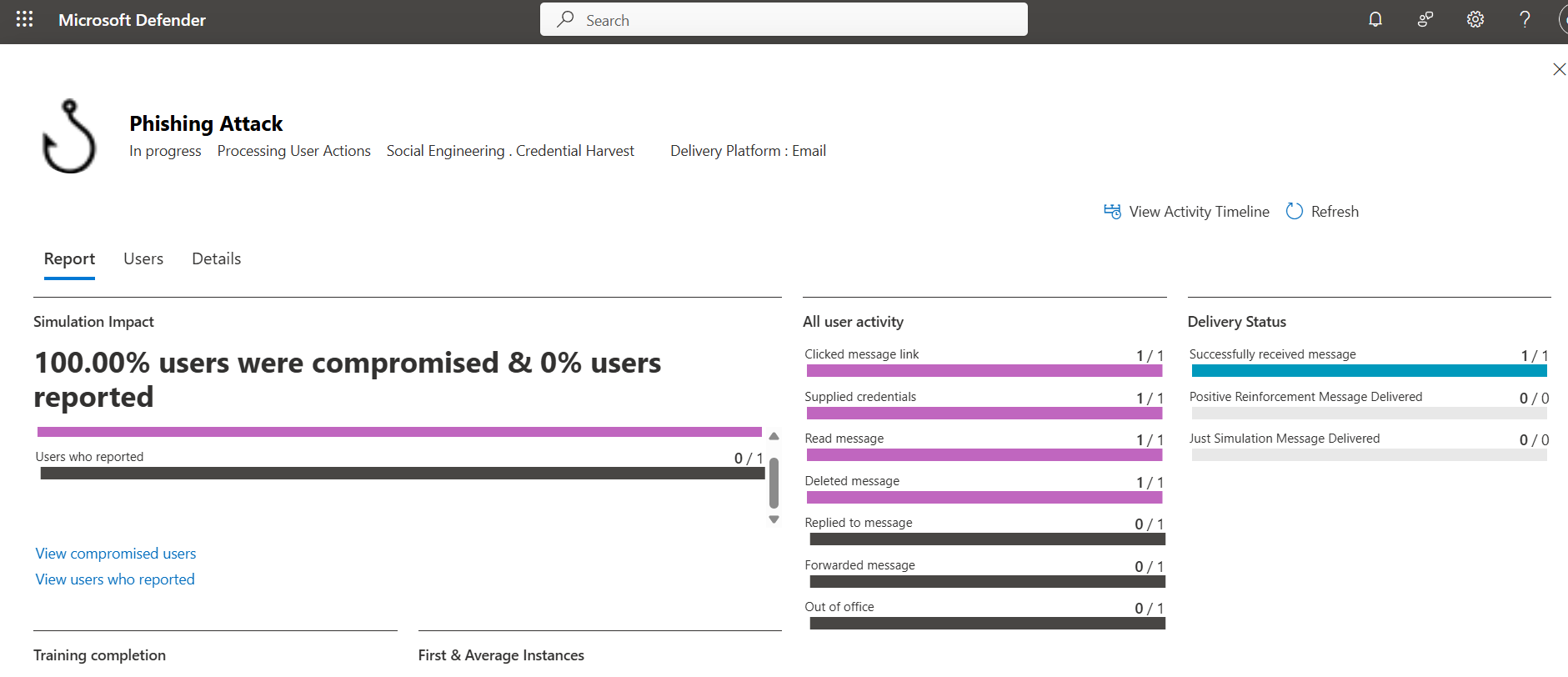
**Phishing email screenshot:**



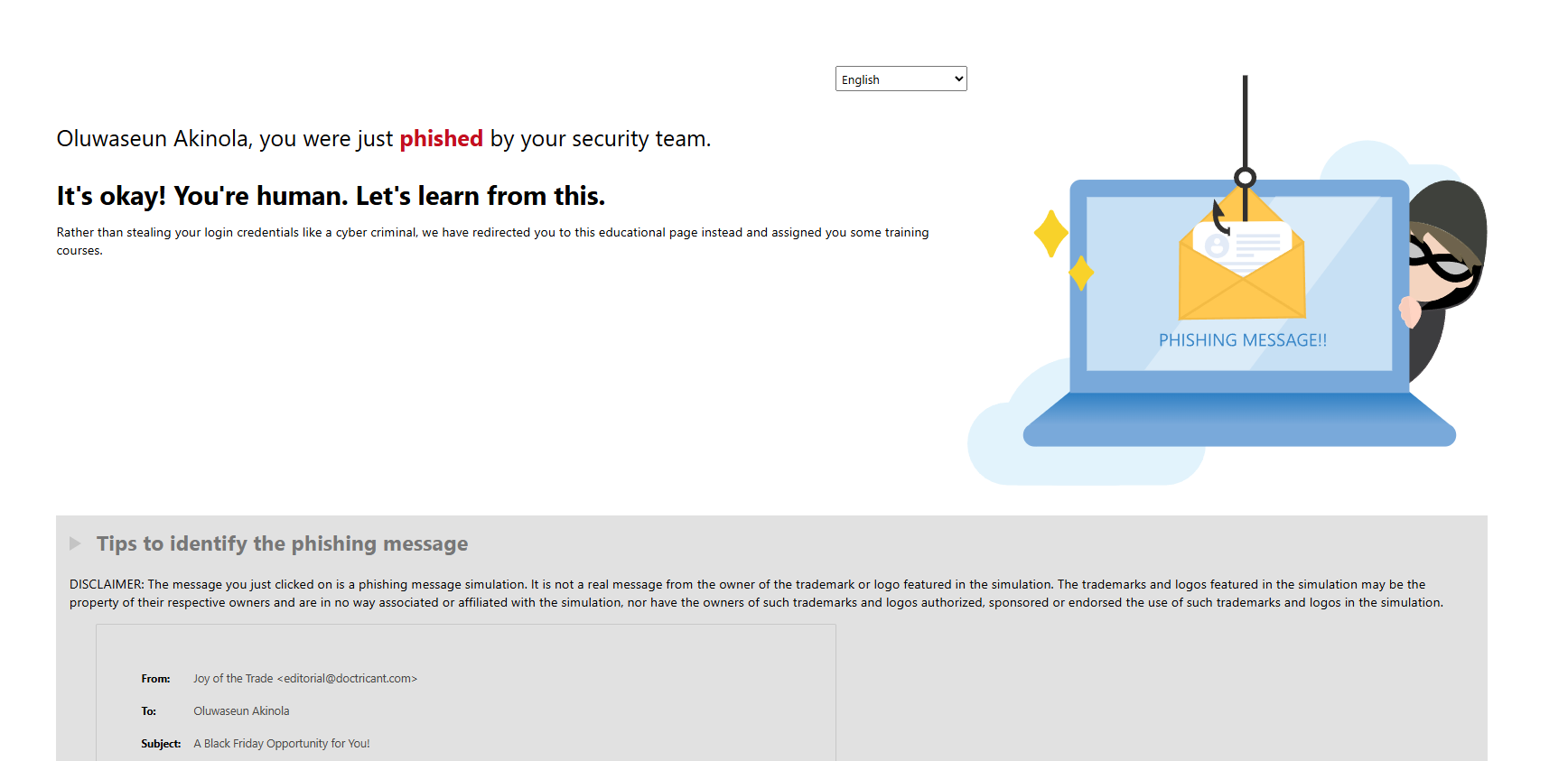
**Screenshot showing user was compromised:**



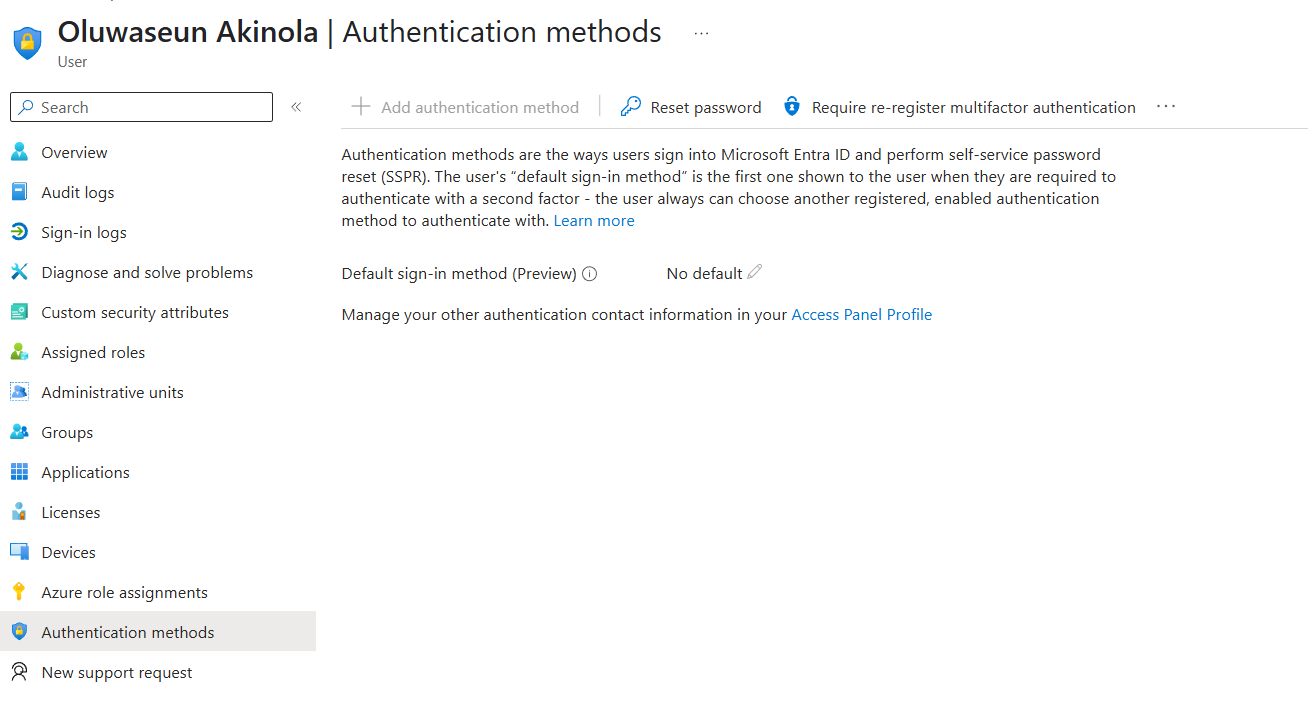
**Simulation report screenshot:**

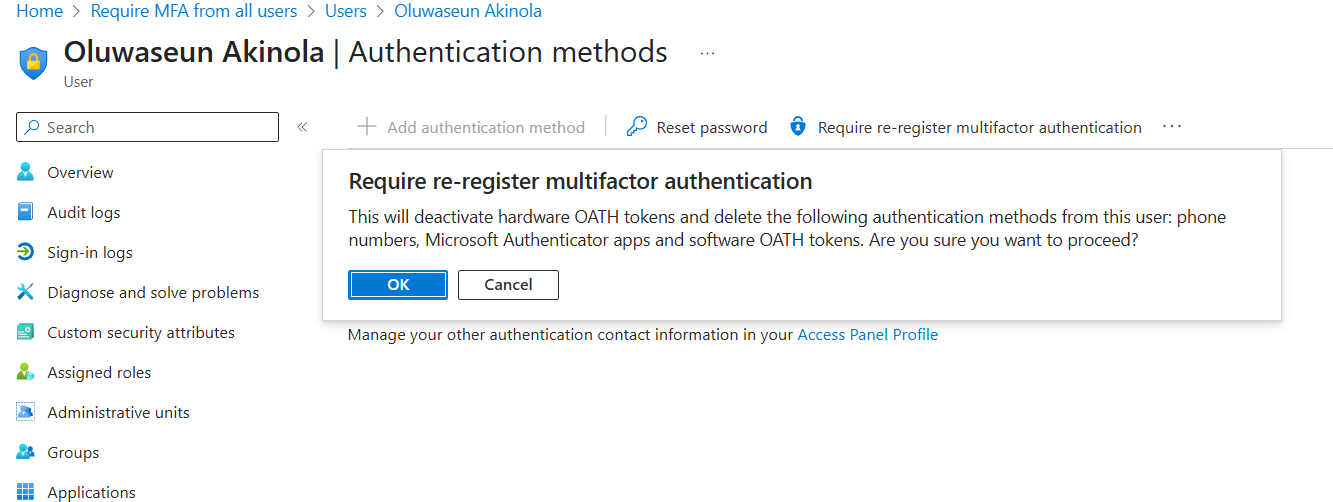


**Screenshot showing user is redirected to a page for tips on phishing attacks:**



**Reset passwords/Revoke user session/Require MFA Re-registration/Assign Training or remind the user.**





**Recovery Actions Taken**

Following the identification of the compromised account, a series of manual recovery actions were performed to secure the account and align with NIST 800-61 best practices:

All active sessions for Oluwaseun Akinola were revoked using Microsoft Entra, immediately terminating any ongoing access to Microsoft 365 services.

A forced password reset was executed to invalidate credentials submitted during the phishing simulation. The user was required to change their password at the next sign-in.

Multi-factor authentication (MFA) was reset, requiring the user to re-register authentication methods to eliminate the risk of token reuse.

The user was directed to complete the phishing training module provided after the simulation, reinforcing secure email habits and phishing awareness.

These steps ensured the account was fully recovered and hardened against future attacks, even though this was a controlled simulation. The manual intervention also revealed areas where automated response policies could be strengthened for faster containment in real incidents.

**Lessons Learned & Recommendations**

During the IAM configuration and incident response setup, one of the key challenges was that risk-based Conditional Access policies (like Sign-In Risk and User Risk) were not immediately available until the appropriate licenses were activated and propagated.

In the incident response simulation, while Microsoft Defender successfully captured phishing interactions, session revocation and user sign-out did not happen automatically, requiring manual intervention. This revealed gaps in automation and response timing that could be critical in a real-world scenario.

**Key Takeaways**

This project highlighted the importance of enforcing least privilege access, regularly reviewing group memberships, and using structured identity roles to reduce risk. Conditional Access policies proved essential in adding extra layers of protection through MFA and location-based restrictions. Additionally, running phishing simulations demonstrated the need for ongoing security awareness among users and the value of having a clear, actionable incident response plan.

Another major takeaway was that tools like Microsoft Defender and Entra ID provide great visibility, but proactive configuration and policy fine-tuning are necessary to fully leverage their potential.

**Recommendations for SecureCart Inc.**

To further strengthen its cloud security posture, SecureCart Inc. should consider the following:

Automate response actions using Microsoft Sentinel or Defender for Identity to respond faster to threats such as account compromise or lateral movement.

Expand IAM audits to include guest access reviews, inactive account cleanups, and periodic group membership validation.

Strengthen Conditional Access policies by combining sign-in risk, user risk, device compliance, and real-time monitoring.

Roll out regular phishing simulations and awareness training to keep users alert and engaged with safe cybersecurity practices.

Develop a centralized incident response dashboard that integrates alerts, logs, and recommendations for faster threat triage.