

PHISHING INCIDENT REPORT

Prepared by: Zakeria Daniels

Date: (December 2,2025)

SUMMARY

A phishing email was reported by a user and confirmed to contain a credential-harvesting link. The attacker attempted unauthorized access to the user's account using stolen credentials.

TIMELINE OF EVENTS

- 09:12 AM – User reported suspicious email
- 09:20 AM – Email analyzed; malicious URL identified
- 09:25 AM – Account login attempt from foreign IP detected
- 09:27 AM – Compromised account disabled
- 09:40 AM – Malicious inbox rules removed
- 10:00 AM – User account restored with MFA reset

INDICATORS OF COMPROMISE (IOCs)

- Malicious URL: [http://secure-login-authenticate\[.\]com](http://secure-login-authenticate[.]com)
- Attacker IP: 185.244.36.12
- File Hash (if applicable): SHA256: (placeholder)
- “Impossible travel” login pattern

ACTIONS TAKEN

- Disabled compromised account
- Revoked active sessions
- Blocked malicious domain and URL
- Removed malicious forwarding inbox rules
- Reset password and MFA registration
- Verified identity with user

RECOVERY

- Restored mailbox access
- Verified no unauthorized emails were sent
- Confirmed MFA login was functioning normally

- Monitored account for 72 hours

RECOMMENDATIONS

- Improve phishing email filter rules
- Provide targeted user awareness training
- Add new IOCs to block list
- Update NIST playbook with findings