BEC Incident Report

Business Email Compromise: Simulated Incident Report

Summary:

A phishing email led to credential theft resulting in unauthorized mailbox access.

Timeline:

- User received invoice-themed phishing email.
- User entered credentials into fake login page.
- Attacker attempted MFA prompts (fatigue attack).
- Token replay observed from unfamiliar IP.
- Inbox rule created for auto-forwarding.
- MailItemsAccessed events confirmed data exfiltration.

Actions Taken:

- Revoked user sessions and tokens.
- Reset password and enforced MFA.
- Removed malicious inbox rules.
- Blocked malicious IP addresses.
- Conducted full audit of account activity.

Outcome:

Account secured. No financial loss.