Compromised Account Action List Example

Immediate Actions

1. Reset account password and enable multi-factor authentication (MFA).
2. Sign out all sessions and invalidate all tokens for the account.
3. Review recent security-related activities (logins, password resets, changes).

Investigation Steps

1. Identify method of compromise (phishing, malware, credential reuse, etc.).
2. Check for unauthorized changes, sent emails, or activities performed by the account.
3. Scan connected devices for malware or unusual activity.

Containment and Recovery

1. Remove unauthorized access (e.g., revoke suspicious app permissions or access).
2. Restore altered or deleted data from backups, if necessary.
3. Notify relevant stakeholders and, if appropriate, affected contacts.

Preventive Actions

- Educate user(s) on safe password practices and account security.
- Ensure that MFA is enforced and active.
- Review and enhance security policies as needed.