OFFICE OF
INFORMATION TECHNOLOGY
STEVENSON UNIVERSITY

Stevenson University Information Security Incident Response Playbook: Compromised Accounts

Last Updated: January 10, 2025

Purpose: This playbook describes the steps to determine how to handle user accounts that may have been compromised.

Procedure

1. Triage.
    a. Here are some of the indications of a compromised account and their risk levels:

	High risk	Medium risk	Low risk
Azure Active Directory Risk Events or Microsoft Cloud Application Security (MCAS) - *Automated notifications sent to Information Security and Network & Infrastructure teams.*	1. User with leaked credentials 2. Confirmed login from suspicious location. (See section b. ii.)	1. Alert for impossible travel 2. Alert for sign-ins from atypical/unfamiliar locations (Azure) or infrequent country (MCAS) 3. Alert for Suspicious session (MCAS)	1. Sign-in from infected device 2. Sign-ins from anonymous IPs
OIT phishing investigation – credential harvesting attempt.	User confirms they entered credentials.	User confirms reading but cannon confirm/recall entering credentials	User confirms they did not read and/or enter credentials
Other source or report of account compromise – law enforcement, other security group (REN-ISAC), media reports, etc. Also review related IR Playbook: Third Party Data Exposure	Any outside report needs to be reviewed by OIT.	Reports from credible groups should start at medium, then investigated by OIT.	Reports from unknown groups or individuals

    b. Tools
        i. Azure Risky Users
        ii. Microsoft Cloud Application Security (MCAS)
        iii. O365 Block All Access to All Apps group
2. Response actions.
    a. High risk. The following actions should occur once an account has been identified as high risk for compromise:
        i. Reset the account
            1. Disable and change password in Active Directory
                a. Admin will add note in the Phones/Notes field in the AD User Object. This is then displayed in the "User Changelog" field of the ADcheck tool used by OIT to look at user accounts.

2. Kill active sessions in Office365.
3. Re-enable the account

ii. Notify user via Web Helpdesk ticket.

1. Initially set no notification to client's Stevenson address and add Swareemail. This is to prevent any email notification from being sent to the compromised account.
2. See Compromised Account Communication Templates for details to put in ticket.

b. Medium risk:

i. Additional investigation by OIT may be required, such as reviewing O365 security logs, content of phishing emails, etc. Some typical types:

1. Impossible travel from mobile device IPv6
2. Personal VPN use
3. Failed attempts from unfamiliar or malicious IPs

ii. An OIT director approval needed to either escalate to high risk or downgrade to low risk. For example, a Microsoft alert for impossible travel could be a false positive, so it is initially a medium risk. If OIT confirms it is a valid malicious login, a director will escalate to high risk. If it's a false positive, downgrade to low risk.

iii. Notify user via Web Helpdesk ticket. See Compromised Account Communication Templates for details to put in ticket.

c. Low risk. No actions are required.