Phishing & Compromised Account Policy

This policy applies to students, staff, faculty, and other members of the Siena Heights University community with an active account. The policy describes steps IT Services will take to ensure the security of accounts and education of community members when they are compromised.

Actions Towards Securing a Compromised Account

When an account is compromised, IT Services will take proactive measures towards securing the account from the malicious attacker. These measures include:

- Resetting the account password.
- Initiating a sign-out for all active Microsoft365 sessions.
- Blocking the ability to send emails from the compromised email account (Microsoft security measure).

Steps that will be taken after the account is secured and the user is contacted are as follows:

- The user will have their password reset through our help desk.
- The email account will be unblocked within 1 hour (Microsoft takes a minimum of 1 hour to do this).
- IT Services will investigate the cause and scope of the attack and notify affected users.
    - This may include identifying users that responded to any malicious emails from the compromised account
    - This may include running a simple report with information on emails sent from the compromised account.
- IT Services will enroll affected users into a short 5-minute Phishing Training course provided through InfoSecIQ.
- IT Services will add the account and notes to an internal system to better track patterns and prevent further security incidents.

Educating Users Affected by a Compromised Account

Students, Staff, and Faculty who have responded to a compromised account, or have had their account compromised, will be enrolled to a short 5-minute Phishing Training course provided through InfoSecIQ. This course is in addition to the normal Faculty and Staff training course(s) provided by IT Services. This course will be optional but highly recommended for users to take as it helps identify compromised accounts and phishing emails.

Users who have been compromised two (2) or more times will be required to take the 5-minute course before their account is re-enabled. This is to ensure the security of their account and online safety of their peers, along with upholding the reputation of Siena Heights University[1].

Further incidents beyond will require the user to meet with a representative from IT Services to discuss further measures on securing their account. These measures can include enabling 2-factor authentication for the account.

[1] – Compromised accounts often send phishing and spam emails to other organizations and institutions. Having this occur too often may tarnish or decrease the reputation and standing held by Siena Heights University. If Siena Heights University accounts are compromised too often, Microsoft may also suspend the account(s) indefinitely.