OFFICE OF INFORMATION TECHNOLOGY
STEVENSON UNIVERSITY

Stevenson University Information Security Incident Response Playbook: Third Party Data Exposure Notifications

Last Updated: January 10, 2025

OFFICE OF INFORMATION TECHNOLOGY
STEVENSON UNIVERSITY

Purpose. This playbook describes the steps to determine how to handle notifications regarding data exposures from third party services that have a possible relationship with Stevenson accounts, mainly where Stevenson email accounts were used to register for third party services.

Procedure

1. Triage.
    a. Source of report.
        i. The following are known, reputable sources:
            1. Have I Been Pwned: https://haveibeenpwned.com/
            2. Research and Education Networks Information Sharing and Analysis Center (REN-ISAC)
        ii. Other sources will need to be evaluated by an OIT director for credibility.
    b. Breach risk factors. The following areas should be considered to determine the appropriate risk level:

Item	High	Medium	Low
Time between breach and notification	Less than 6 months	6 months – 2 years	More than 2 years
Number of accounts	1000+	11-999	1-10
Did third party notify users?	Users were not notified	Unconfirmed	Users were notified
Sensitivity of exposed information	Passwords, social security numbers, credit card numbers, birth dates	Personal information – identities of relatives, salary, memberships	Widely available information – names, email, addresses, phones
State of exposed information (typically passwords)	No encryption	Weak encryption (MD5, RC4, SHA- 1)	Strong encryption (bcrypt, salted, etc)
How relevant is the service to legitimate university activities?	Strong relevance	Some relevance	No relevance

Correlation with other sources	Confirmed correlation from other 3rd party	Some correlation, such as by the owner	No other correlation

1. Response actions.
    a. An OIT director will review the individual factors to make an overall determination regarding the risk.
    b. Follow the IR Playbook for Compromised Accounts for the response actions based on the risk rating.