OFFICE OF
INFORMATION TECHNOLOGY
STEVENSON UNIVERSITY

Stevenson University Information Security Incident Response Playbook: Potentially Malicious Emails

Last Updated: January 10, 2025

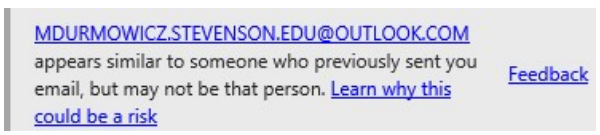
Information Security Incident Response Playbook:

Potentially malicious emails

1. Purpose. This playbook describes the steps to determine how to handle potentially malicious emails within Stevenson University's email system.
2. Procedure
    a. Use the following tools to triage any suspected emails,
        i. The original submission to Helpdesk mailbox. Quick triage. Provides initial data: Date/time, sender, subject, etc.
        ii. M365 Security Compliance Content search.
            1. Some possible search criteria
                a. Sender SMTP
                b. Sender domain only, especially @gmail.com
                c. Subject line
            2. Search results. Can download original email w/headers if needed.
        iii. M365 Security Compliance Content search report. Things to look at:
            1. Original path. Shows inbox, junk, etc.
            2. Location name: Recipient smtp addresses to send notification
            3. Recipients in CC line: May need to add
            4. Is Read: In case of malicious link or attachment
        iv. VirusTotal (https://www.virustotal.com/gui/home/url) Nice to check out suspicious urls without having to click on them. Provides good detailed report.
        v. Basic internet search (Open Source Intel – OSINT). Simply search the subject line, keywords, etc.

            Often there's info on the specific of the phishing attack.

        vi. M365 Threat Management (more research is required)
            1. Automated investigations: https://protection.office.com/airinvestigation
            2. Campaigns: https://protection.office.com/campaigns
        vii. Abnormal Security: https://abnormalsecurity.com/
            1. Search and Respond
            2. Remediate as needed (sends email to their "Recover Deleted Items")
                a. Submit missed attack or campaign for review by Abnormal Security
    b. Using information from the tools determine:
        i. How many people received the email?
            1. Threshold?
        ii. Does the email contain any malicious content including:
            1. Link or attachment.
            2. Impersonation of a Stevenson individual or organization
            3. Threat. Includes extortion attempts against the recipient.
        iii. Has there been any automated detection of the emails with Office365 Security Center?
        iv. Was the email delivered to the InBox or Junk folder?
        v. Was the email tagged with any warning, such as anti-phishing impersonation:
            1. Specific users (anti-impersonation list)



2. General domain spoofing:

vi. Typical types of phishing campaigns:
1. Gift card scams with impersonation.
2. Document sharing from hijacks Google or Microsoft accounts.
3. Fake IT or account notifications
4. Paycheck redirects with impersonation

c. Determine follow-up actions.
i. Notification to recipients:
1. Subject: OIT Alert: Phishing {simple description of phishing email}
2. Send to helpdesk@Stevenson.edu
3. CC: CIO, Director of Networks and Infrastructure, Director of Technology Services, Director of User Support & Engagement.
4. If impersonation was involved, CC: the person impersonated.
5. BCC: All recipients of the message.
6. Include appropriate information about the phishing and any actions needed if they were a victim, such as password reset.
7. Example (see others in Helpdesk mailbox)

> To recipients
>
> Subject: OIT Alert: Phishing xxxxx
>
> You are receiving this alert because you were the recipient of a suspicious email with the
>
> subject line “PART TIME JOB OFFER”
>
> The sender used a Stevenson faculty member’s email account to send the message to a
>
> large number of people at Stevenson.
>
> Thanks to several of you for reporting this.
>
> This is a scam. If you responded, do not respond any further. You can delete all these emails.
>
> If you have any concerns, please open a ticket with OIT:
> https://helpdesk.stevenson.edu

ii. Submit sample email:
1. O365: https://protection.office.com/reportsubmission
2. Google: https://support.google.com/mail/contact/abuse

iii. Additional actions not typically required and requiring OIT director approval.
1. Notification to other groups (administration, campus-wide, etc.).
2. Blocking email addresses. In general, the blocking of specific email addresses used by bad actors is not required. Bad actors rarely re-use the same email address.

3. Purging. Generally purging not effective unless done very quickly. Can be done via PowerShell using results of M365 Content Search.