

- 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 redirect with impersonation
- c. Determine follow-up actions.
  - i. Notification to recipients:
    - 1. Subject: OIT Alert: Phishing (simple description of phishing email)
    - 2. Send to SecureIT@Stevenson.edu
    - 3. CC. ClO, 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 SecureIT mailbox)

To recipients

- 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.