Procedures for removing email post-delivery

Objective

In accordance with the Information Security and Acceptable Use Policy (UTDBP3096) and established Incident Response Procedures maintained within the Information Security Office (ISO), this procedure serves to further explain risk mitigation actions that may be performed when a malicious email has been detected after delivery to users. The procedure specifically explains conditions whereby post-delivery filtering will be applied because pre-delivery filtering did not completely detect and quarantine malicious email. In additional to explaining the appropriate post-delivery filtering method, the approval authority is also listed.

Process

1. Automated filtering tools perform 24x7 analysis of emails as they reach the UT Dallas domain before delivery to users; if conditions are met which are indicative of probable malicious behavior, the automated filtering tools delete, quarantine, tag, or otherwise handle the email message. This process significantly reduces risk but does not identify all malicious emails.

2. On occasion, malicious emails do arrive at user inboxes. Conscientious users report such emails to the ISO for investigation. When ISO investigation concludes, there is a high confidence that whether the email is, in fact, malicious.

3. In the event that the ISO investigation of a reported email concludes that malicious intent poses a risk to UT Dallas assets, operations, or users, certain steps may be recommended by the ISO to mitigate such risk:
    - Firewall updates to limit access to malicious links contained in the email
    - Anti-malware software updates associated with malware carried by the email
    - Communication to users, often by email, to inform them of the malicious campaign
    - Post-delivery actions, as detailed in the table above.

4. The ISO performs and/or coordinates the appropriate mitigation steps listed above.

5. Documentation of actions performed will be retained for at least 1 year to provide historical reference and address questions and concerns of users.

Background

Several user types, such as employees, student employees, and students, use UT Dallas email resources within a single Microsoft 365 environment. This environment is provided to user for the purpose of enabling UT Dallas work and study. This single consolidated email environment makes it unrealistic to take actions strictly limited to a user group, such as employees only. Therefore, the response plans are based on the intrinsic risk of the malicious email types, rather

than user type. Post-delivery filtering will be facilitated by the Microsoft 365 toolset, which includes built-in functionality for such incident response. The actions offered by the system include:

- Move to Junk – moves the malicious email to the user's Junk Email folder
- Move to Deleted Items – moves the malicious email to user's Deleted Items folder
- Soft Delete – user has approximately 30 days to restore the deleted malicious email
- Hard Delete – permanently deletes the malicious email; user loses access to it

Common Malicious Email Events

Security Exposure	Incident Response Action	Primary Requestor	Request Approver	Documentation Requirements
Unsolicited Marketing aka. Spam	No Central Action Taken – Direct User to Self Service	N/A	N/A	N/A
Imitation HR Service Providers	Soft Delete	HR Department	Deputy CISO / CISO	Document email and actions
Job Scam from external sender	Soft Delete	Incident Response Analyst	ISO Manager	Document email and actions
Job Scam from utdallas.edu sender	Hard Delete	Incident Response Analyst	ISO Manager	Document email and actions
Leadership Impersonation / Gift Cards	Hard Delete	Incident Response Analyst / Impersonated Leader	ISO Manager	Document email and actions
Stolen Password / Data Exfiltration	Hard Delete	Incident Response Analyst	ISO Manager	Document email and actions
Ransomware Malware	Hard Delete	Incident Response Analyst	ISO Manager	Document email and actions
Other Malware	Hard Delete	Incident Response Analyst	ISO Manager	Document email and actions
Unintentional Mistakes / Leaked Controlled Data	Hard Delete	Department Head	Deputy CISO / CISO	Document email and actions