HOWDY!

DSA IT Liaisons Communications Committee

12/3/2019
Agenda

- Tech Tip: Proofpoint Spam Filtering
- Inventory Management Process
- Cloud Computing SAP
- This month in DoIT
- Q&A
Proof point Spam Filtering
Tech Tip: Proof point Spam Filtering

• Texas A&M central email servers use Proof point to identify and block or quarantine unsolicited email (spam)
• Recipients with quarantined messages will receive a bi-daily quarantine digest
• From the digest, messages can be released or deleted, and senders can be whitelisted or blacklisted
• Recipients can access their profile and change their spam detection from the default to more or less aggressive spam detection
The messages in your personal Digest represent emails that have been filtered and sorted into different categories, giving you an opportunity to take action on them. Click the link in the Subject column to view the message.

The emails listed in this section have been placed in your personal Quarantine. Click Release to deliver the email to your inbox. To continue to receive future emails from the sender, click Allow Sender. To report messages that are not spam but are included in the Spam - Quarantined section, click Not Spam.

<table>
<thead>
<tr>
<th>Size</th>
<th>From</th>
<th>Subject</th>
<th>Date</th>
<th>Action</th>
<th>Subject</th>
<th>Date</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>14KB</td>
<td>@Insightsforprofessionals.com</td>
<td>Carl, 10 questions to ask yourself about Office 365 deployment...</td>
<td>2019-12-02 09:11:59</td>
<td>Release  Release and Allow</td>
<td>Carl, the changing face of leadership...</td>
<td>2019-11-26 13:58:05</td>
<td>Release  Release and Allow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Sender Block Sender Delete</td>
<td></td>
<td></td>
<td>Delete Not Spam</td>
</tr>
<tr>
<td>13KB</td>
<td>@Insightsforprofessionals.com</td>
<td>Carl, the 3 criteria of a successful intelligent workplace...</td>
<td>2019-12-27 09:18:09</td>
<td>Release  Release and Allow</td>
<td>Carl, here's 3 top tips for improving team collaboration...</td>
<td>2019-11-26 15:53:24</td>
<td>Release  Release and Allow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Sender Block Sender Delete</td>
<td></td>
<td></td>
<td>Delete Not Spam</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Sender Block Sender Delete</td>
<td></td>
<td></td>
<td>Delete Not Spam</td>
</tr>
<tr>
<td>12KB</td>
<td>@Insightsforprofessionals.com</td>
<td>Carl, are hackers listening in on your conversations?</td>
<td>2019-11-22 09:08:27</td>
<td>Release  Release and Allow</td>
<td>Carl, here's 5 steps to creating a unified communications strategy that works...</td>
<td>2019-11-21 15:15:05</td>
<td>Release  Release and Allow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Sender Block Sender Delete</td>
<td></td>
<td></td>
<td>Delete Not Spam</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Sender Block Sender Delete</td>
<td></td>
<td></td>
<td>Delete Not Spam</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Sender Block Sender Delete</td>
<td></td>
<td></td>
<td>Delete Not Spam</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Sender Block Sender Delete</td>
<td></td>
<td></td>
<td>Delete Not Spam</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Sender Block Sender Delete</td>
<td></td>
<td></td>
<td>Delete Not Spam</td>
</tr>
</tbody>
</table>
Understanding Quarantine Actions

- Release an email to your inbox, - future emails will still be quarantined
- Releases an email to your inbox, and adds to “safe-ender” list
- Adds sender to Block List
- Delete an email from quarantine list
- Releases an email to your inbox - Updates quarantine rules to allow similar content in the future
Updating Proof point Settings

Sends a quarantine digest on demand

Sends an email to your inbox, listing your safe/blocked users

Logs you on to Proofpoint to manage your settings...
Changing Proof point Settings
Inventory Management Process

Cameron Baker
Inventory Management Process

The goal of the DoIT Inventory Management Process is to allow both DoIT and its DSA counterparts to ensure that inventoried IT assets and related work are effectively tracked and provide transparency related to asset location.

This ensures that:

• Assets are accounted for
• Documentation is created for asset movement
• Reports on assets can be provided if requested
• Minimizes the loss of assets due to mishandling or lack of tracking
• Increases transparency with customers inventory location
• Assists customers with the fiduciary management of assets
Inventory Management Process: Roles

Department Asset Manager

- Process the ordering of IT assets as part of the department’s internal business purchase process, working in conjunction with the DoIT Asset Manager
- Notify the DoIT Service Desk in writing, 5 business days prior to, when an item needs to be moved
- Certify their inventory as a part of annual compliance
- Maintain IT asset records in Canopy when IT assets are moved
Inventory Management Process: Roles

DoIT Asset Manager

- Ensures all DoIT staff log and track all equipment in temporary DoIT possession while work is being performed on an asset
- Provide updates, upon request, to customers about the location of their assets while in temporary DoIT possession, including:
  - Pickup
  - Working location
  - Storage location
  - Deploy/return location
- To estimate time that an IT asset will be in DoIT’s possession
- Assists in the acquisition of inventoried technology assets
- Improves/Changes process as needed
- Will maintain a list of Dept. Asset Managers
Inventory Management Process: Workflows

**Acquisition**

DoIT
- Receive bulk shipments
- Notify department when assets received
- Unpack shipments to verify serial numbers
- Verify Dept. asset manager places asset tags

Dept. Asset Manager
- verifies IT assets and tags them with TAMU asset control sticker
- updates asset information in FAMIS/Canopy
Inventory Management Process: Workflows

Deployment & Moves

DoIT Asset Manager/Service Desk
- tags IT assets with Inventory Control Form
- coordinates deployments and moves with department
- provides information via ticket about updated location

Dept. Asset Manager
- coordinates with DoIT on scheduling of deployments and moves
- provides DoIT with new location for asset
- updates asset information in FAMIS/Canopy
- stores items for surplus and coordinates surplus with Property Mgmt.
Inventory Management Process: Workflows

Temporary Move (break-fix at Service Desk)

DoIT Service Desk
- tags IT assets with Inventory Control Form
- communicates with department/user if vendor warranty work is required
- logs status updates and information in ticket

Dept. User
- verifies work is completed upon return of asset
Inventory Management Process: Workflows

Annual Inventory Certification

Dept. Asset Manager
- verifies IT asset location and certifies physical inventory
- updates asset information in FAMIS/Canopy
- can request asset information to help locate asset via ticket

DoIT Asset Manager
- attempts to provide historical information available related to asset location upon request
Cloud Computing SAP

Anthony Schneider
Cloud Computing SAP

• 29.01.03.M0.13 Information Resources – Cloud Computing Services
  – Phased in, applies to SaaS Sept 1, 2020.

• Applies to:
  – Infrastructure as a Service (IaaS) - Amazon AWS, Microsoft Azure
  – Platform as a Service (PaaS) - Amazon Elastic Beanstalk, Windows Azure
  – Software as a Service (SaaS) - Almost everything not hosted on campus

• Applies to:
  – High or Moderate Impact Information Resources
• High Impact Information Resource
  – Information Resources whose loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. Such an event could:
    • (A) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
    • (B) result in major damage to organizational assets;
    • (C) result in major financial loss; or
    • (D) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

• Moderate Impact Information Resource
  – Information Resources whose loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. Such an event could:
    • (A) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
    • (B) result in significant damage to organizational assets;
    • (C) result in significant financial loss; or
    • (D) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
Cloud Computing SAP

• **Notable Requirements**
  – Approved by CIO or designee
  – CIO to maintain a list of approved providers on their website
  – Follows all TAMU Rules, SAPS, and IT Controls (Contracts)
  – No personal Cloud Computing Services can be used to store Restricted or Confidential data

• **How to get Approved**
  • FedRAMP automatically approved ([FedRAMP official website](https://fedramp.gov))
  • HECVAT (Higher Education Cloud Vendor Assessment Tool) score
  • TAMU Security Review
This month in DoIT

Anthony Schneider
This month in DoIT

• Successfully Completed West Campus Data Center Move
• Released new StuOrg Online Application for MSC use
• CAPS Consolidation and PnC Implementation underway
• Service Desk/Systems Teams heavily involved in SSB moves
• Candidate reviews started for PM II and SAD II positions
Department Q&A

Anthony Schneider