Policy for Protecting Outgoing Mason E-mail

Introduction

During the last year, a number of Mason e-mail accounts were used maliciously to send out SPAM and Phishing e-mail attacks. These incidents hurt the reputation of the university and cause our messaging domain to be blocked by Internet Service Providers including Sprint, Verizon and AT&T.

In order to constrain, identify and repair compromised e-mail accounts at Mason, the ITU deployed outbound e-mail scanning and filtering (based on the parameters detailed in the table below) in a very similar manner that inbound e-mail is currently scanned and filtered. The e-mail team implemented the required system changes on the servers and no end-user configuration changes are required.

The Benefits of Implementing Outbound Filtering:
- Mason can monitor outbound e-mail traffic more effectively.
- ITU e-mail engineers can limit the amount of Phishing e-mail sent out from the Mason network and reduce the chance that Internet Service Providers or other domains will add Mason’s IP address to a block list.

A Comparison of Inbound and Outbound Filtering

The following is a comparison of the actions taken to protect inbound and outbound mail.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Current Inbound</th>
<th>New Outbound</th>
<th>Current Action Taken on Inbound E-mail</th>
<th>Outbound Action Taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus Checking</td>
<td>Yes</td>
<td>Yes</td>
<td>Messages containing a virus are deleted. No notification is made to the sender or intended recipient.</td>
<td>Messages containing a virus will be deleted. A reply will be sent to the sender indicating their computer is infected &amp; their e-mail account will be temporarily disabled until the virus is remediated. Information about the message will be retained and sent to the IT Security Office. Compromised accounts will be disabled until the owner speaks with ITU Support, changes their password, and (if they are Faculty/Staff) speak with the Security Office to ensure there is no highly sensitive information on their computer.</td>
</tr>
<tr>
<td>Maximum Simultaneous Connections per IP (Likely the result of a Phishing or SPAM e-mail)</td>
<td>5000</td>
<td>10</td>
<td>Connection attempts that exceed the threshold are blocked.</td>
<td>Connection attempts that exceed the threshold will be blocked. The e-mail team will review activity logs each workday in order to identify potentially compromised accounts. Compromised accounts will be disabled until the owner speaks with ITU Support, changes their password, and (if they are Faculty/Staff) speak with the Security Office to ensure there is no highly sensitive information on their computer.</td>
</tr>
</tbody>
</table>
Maximum Messages per Connection

( likely the result of a Phishing or SPAM e-mail)

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5000</td>
<td>500</td>
<td></td>
</tr>
<tr>
<td>Message attempts that exceed the threshold are blocked.</td>
<td>Message attempts that exceed the threshold will be blocked. The e-mail team will review activity logs each workday in order to identify potentially compromised accounts. Compromised accounts will be disabled until the owner speaks with ITU Support, changes their password, and (if they are Faculty/Staff) speak with the Security Office to ensure there is no highly sensitive information on their computer. Senders of a legitimate e-mail to more than 500 addresses will be asked to move their list to our listserv service that is exempt from outbound scanning.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Check Message Headers Against a Database of Known Addresses used by Phishers

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Messages with a &quot;reply to&quot; address of a known &quot;Phisher&quot; are discarded.</td>
<td>Messages with a &quot;reply to&quot; address of a known &quot;Phisher&quot; will be deleted. The e-mail team will review activity logs each workday in order to identify potentially compromised accounts. Compromised accounts will be disabled until the owner speaks with ITU Support, changes their password, and (if they are Faculty/Staff) speak with the Security Office to ensure there is no highly sensitive information on their computer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

University Security Procedures for a Compromised E-mail Account

The following is a breakdown of the security procedures that are use to protect the outbound mail of various groups Mason e-mail users.

**Faculty/Staff/Wage**

- Passwords are reset (this will disable the ability to log in to all resources that use the LDAP for authentication, including Patriot Web, Oracle Calendar, and E-mail.
- E-mail accounts are disabled
- IT Security Office (ITSO) personnel contact the individual:
  - to determine the method used to compromise the account
  - if highly sensitive information is on the computer (if the individual works with highly sensitive information, ITSO personnel will determine if data exposure could have occurred)
  - to insure the individual's system is clear of viruses and spyware
  - to educate the individual on security and best practices
- ITSO personnel clear the account and reopen e-mail account
- Individual works with the ITU Support Center to reset their password

**Students residing on Campus**

- Passwords are reset (this will disable the ability to log in to all resources that use the LDAP for authentication, including Patriot Web, Oracle Calendar, and E-mail.
- E-mail accounts are disabled
- ResTechs contact the individual:
  - to determine the method used to compromise the account
  - to insure the individual's system is clear of viruses and spyware
  - to educate the individual on security and best practices
- ResTechs clear the account and ITU Support Center reopens the account
• Individual works with the ITU Support Center to reset their password

Students residing off Campus

• Passwords are reset (this will disable the ability to log in to all resources that use the LDAP for authentication, including Patriot Web, Oracle Calendar, and E-mail.
• E-mail accounts are disabled
• Individuals must contact the ITU Support Center. The ITU Support Center works with the individual:
  o to request the individual scan their system for viruses and spyware
  o to educate the individual on security and best practices
• ResTechs clear the account and ITU Support Center reopens the account
• Individual works with the ITU Support Center to reset their password