

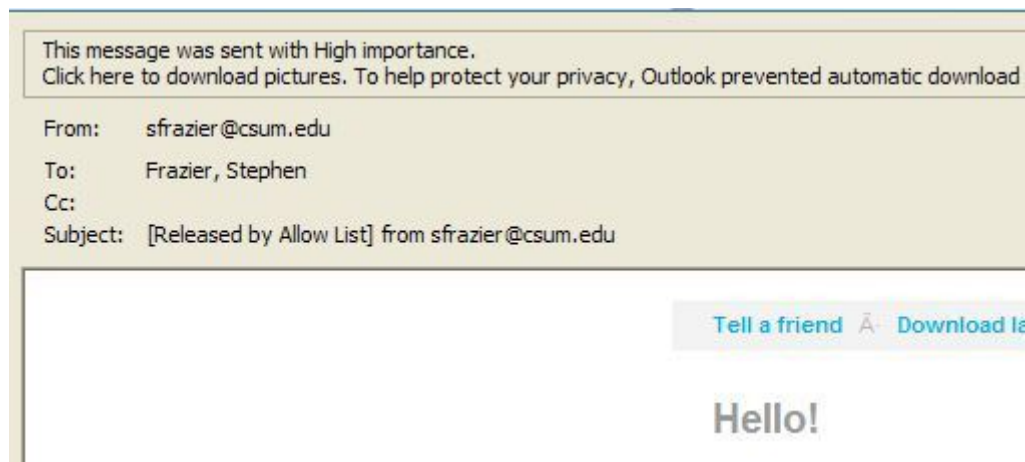


Excessive Amounts of Spam

Are you seeing an excessive amount of spam messages when you open your university email? If so, this usually can be attributed to your personal configuration settings in the SonicWALL institutional spam filter. The SonicWALL is an appliance that sits between the Internet and Cal Maritime's Exchange server. All inbound email traffic to the University must pass through it before reaching the Exchange server.

As an FYI, the SonicWALL spam filter should not be confused with the Junkmail folder that appears in Outlook... they are not the same. Email in the Junkmail folder in Outlook has already passed through the SonicWALL and therefore those messages actually reside on the Exchange server... not the SonicWALL.

The picture below depicts a portion of a message found in sfrazier's Outlook Inbox folder. It was a spam message that should have been blocked by the SonicWALL appliance. Why did the SonicWALL appliance permit it to be passed through to this user's Inbox?



The header information, as depicted above, is as follows:

From: sfrazier@csum.edu
Sent: Wednesday, April 15, 2009 5:20 PM
To: Frazier, Stephen
Subject: [Released by Allow List] from sfrazier@csum.edu

There are two clues in this header (see the highlighted text shown above) that point to the root cause of the problem.

1. The subject of message includes "[Released by Allow List]."

2. **From:** sfrazier@csum.edu (in some cases, the person's actual name may appear instead of the address). The fact that the recipient is also the sender (which is obviously not the case) indicates that the message was spoofed to appear as though it originated from this user's email address.

“[Released by Allow List]” in the subject line suggests that the filter purposely allowed the spam to be released per this user's personal configuration settings in the SonicWALL filter. The filter releases spam when the recipient's own email address (sfrazier@csum.edu in this case) is included in the list of people who are allowed to send email to him/her.

Each person can add email addresses to his/her list of allowed senders to insure that the filter does not block certain people from sending messages to him/her. When a user clicks on the “unjunk” link for suspect messages in his/her daily “Junk Box Summary” messages, for example, the sender(s) is automatically to this allowed list. This list can grow surprisingly long over time.

In the case we are presenting here, a review of the “People” allowed to send messages in sfrazier's personal settings indeed revealed that his address (sfrazier.csum.edu) was included in his allowed sender list. While it may not be readily apparent how a person's own email address was inadvertently added, it is probably related to the process of unjunking messages.

Reviewing Your List of Allowed Senders

The screenshot displays the SonicWALL Email Security management console. The left sidebar contains navigation options: Junk Box, Anti-Spam, Anti-Phishing (expanded), People (selected), Companies, Lists, Anti-Spam Aggressiveness, Foreign Languages, Settings, Reports & Monitoring, and Downloads. The main content area is titled 'Anti-Spam, Anti-Phishing / People'. It features a 'Blocked' tab and buttons for 'Add', 'Delete Selected', and 'Delete All'. Below these is a table of allowed senders with checkboxes and a search dropdown.

Sender's Email Address
<input type="checkbox"/> sc1716@att.com
<input type="checkbox"/> scalise@sonoma.edu
<input type="checkbox"/> scirl@aol.com
<input type="checkbox"/> scott.metcalf@sun.com
<input type="checkbox"/> scucciuffo@equitrac.com
<input type="checkbox"/> sealink@marlink.com
<input type="checkbox"/> sealink@vizada.com
<input type="checkbox"/> seemant_mathur@campuseai.org
<input type="checkbox"/> sera_nelson@campuseai.org
<input type="checkbox"/> sera_nelson@cleveland.ceainet.campuseai.org
<input type="checkbox"/> sfrazier.cio@gmail.com
<input checked="" type="checkbox"/> sfrazier@csum.edu
<input type="checkbox"/> sfrazier@sonoma.edu

You should periodically review the entries in your allowed list of senders by logging onto to the spam filter (go to <https://mail01.csum.edu>) [notice the “s” in https] and type your windows credentials). After logging on to the SonicWALL, click the “Anti-Spam, Anti-Phishing” option in the panel on the left and then click “People” to see your list of allowed senders. If you find your email address in this list, click the small box beside it and then click the “Delete Selected” button to remove it.

We'd love to hear from you! Please send your questions and comments to HelpDesk@csum.edu. Previous tips are online at: <http://www.csum.edu/IT/tipoftheweek.asp>