

SPAM message protection in blueView collaboration suite

To see **examples** of **SPAM** and **PHISH** messages please view our PHISH document on the Drake.edu/IT page. These will help you understand how to **identify** SPAM and PHISH to protect your identity.



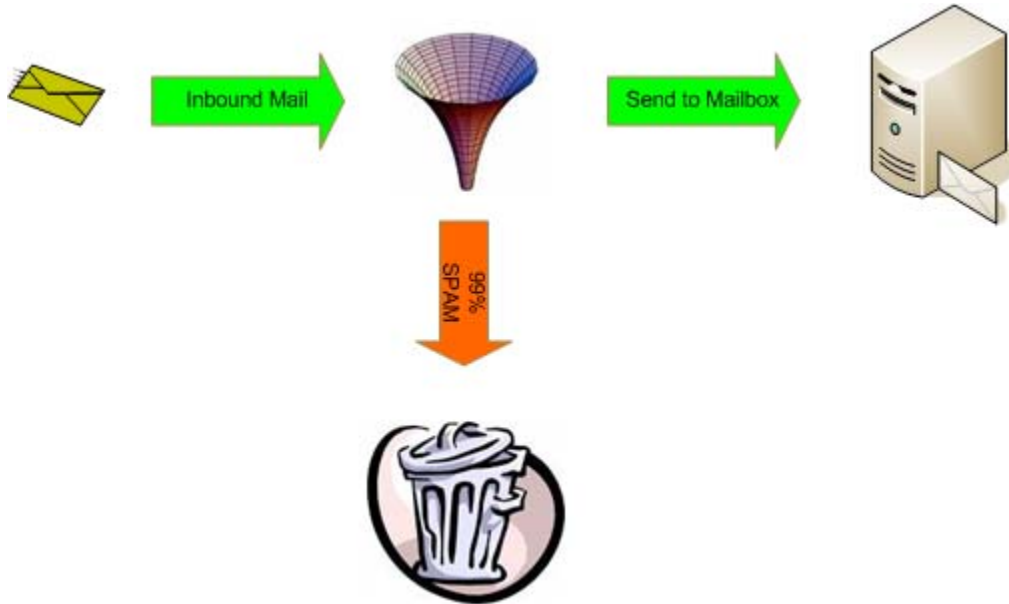
Topics:

- How SPAM is managed in the new system – page 2
- How to validate messages – page 3
- How to reduce SPAM – page 6
- More information about filtering and SPAM – page 7



How SPAM is managed in the blueView collaboration suite

As messages arrive to the Drake network they are scanned by an edge system and examined for 'probability' matches of SPAM and Phish content. If they are 99%+ tagged as spam they are deleted before they reach our network. The rules look for key words and from known addresses and domains.



Messages that do not meet the initial criteria are passed to our internal mail system for further review. Messages that meet 50%-99% are tagged as "Junk" and placed in your "Junk" folder on the server.



It is up to you to review these messages on a regular basis. Some messages are not junk, but have had certain strings, links, or other wording that may have placed them in the folder.

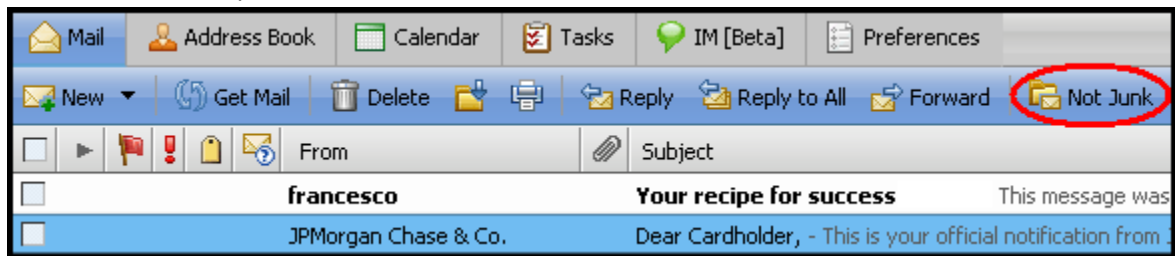
How to Validate SPAM

- Webmail
- Outlook
- Eudora
- Entourage

If a message in the message in the Junk folder is from a valid source or NOT Junk:

Webmail “Junk” folder

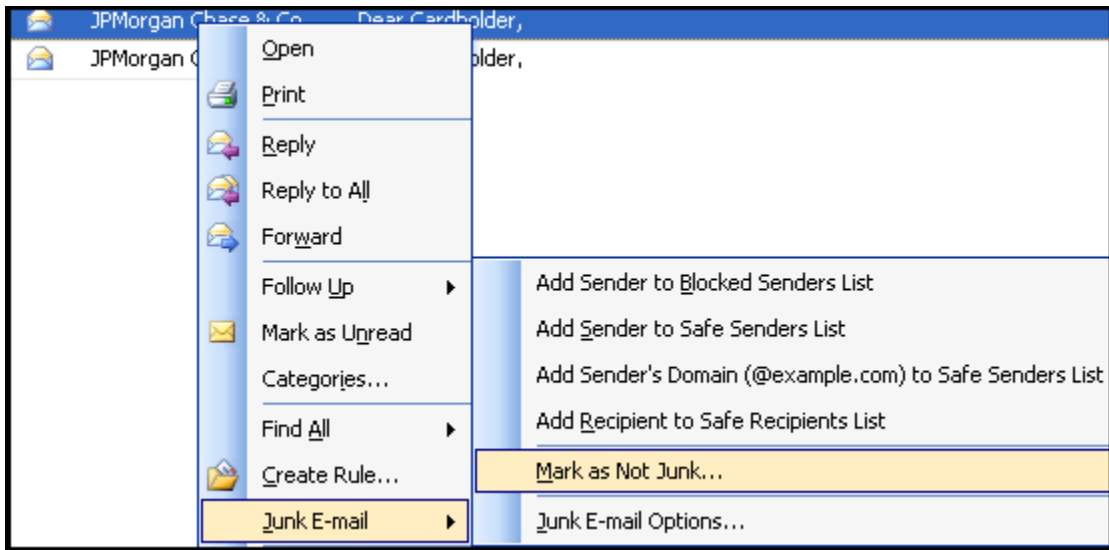
1. Click on the message from the Junk folder to highlight.
2. Click button “Not Junk”
3. The message will be moved to your Inbox and the rules that placed it in Junk will be modified to help reduce this in the future.



Outlook “Junk”

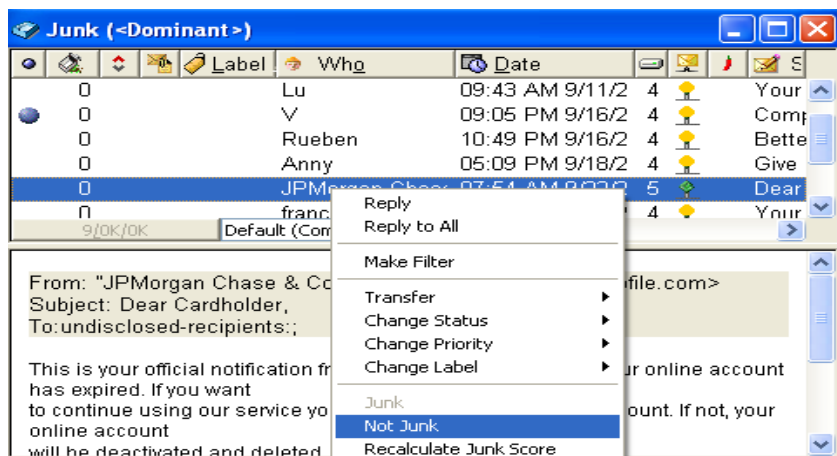
Outlook will use Microsoft rules, in addition to the server, to place suspect mail in the “Junk E-Mail” folder

1. Click on message in the Junk or Junk E-Mail folder to highlight
2. Right click
3. Scroll down to “Junk E-Mail”
4. Scroll over to “Mark as Not Junk”
5. The message will be moved to your Inbox and the rules that placed it in Junk will be modified to help reduce this in the future.



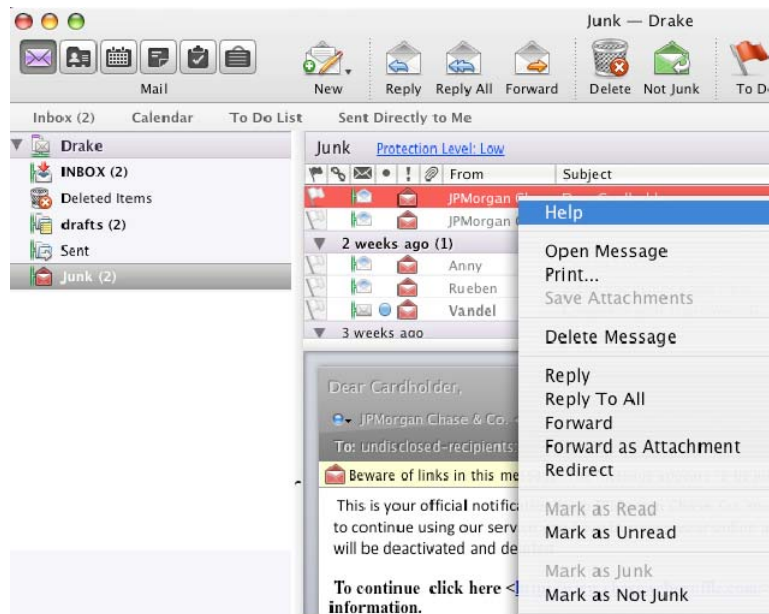
Eudora - It is important to note that some versions of Eudora will not manage mail in a Junk folder without the paid version.

1. Open Junk folder
2. Right click on message
3. Scroll down to Not Junk
4. The message will be moved to your inbox and the rules that placed it in Junk will be modified to help reduce this in the future.



Entourage

1. Open Junk Folder
2. Click on Message
3. Click on "Not Junk" icon on menu bar
or
4. Right click and scroll down and select Mark as Not Junk



How to reduce SPAM

Occasionally a message will appear in your INBOX that you would rather not see. SPAMers use many techniques to pass messages through our validation system. What appears to us visually may not look like SPAM to a system. For example the word "Free" could be sent as "F r_e e" or "f_r 33". Systems cannot pickup all the variations used.

- Webmail
- Outlook
- Eudora
- Entourage

If a message appears in your INBOX that is SPAM or you do not want to receive messages from the sender:

Webmail "Junk" folder



1. Click on the message from the INBOX to highlight.
2. Click on the Junk button in the menu bar

Outlook "Junk"

Outlook will also use Microsoft rules to place suspect mail in the "Junk E-Mail" folder

1. Click on message in the Junk or Junk E-Mail folder to highlight
2. Right click
3. Drag message to "Junk"

Eudora

1. Click on message
2. Right click
3. Scroll to Junk

The message will be moved to the Junk folder. Rules will apply to the system to help prevent further messages like or similar to these.

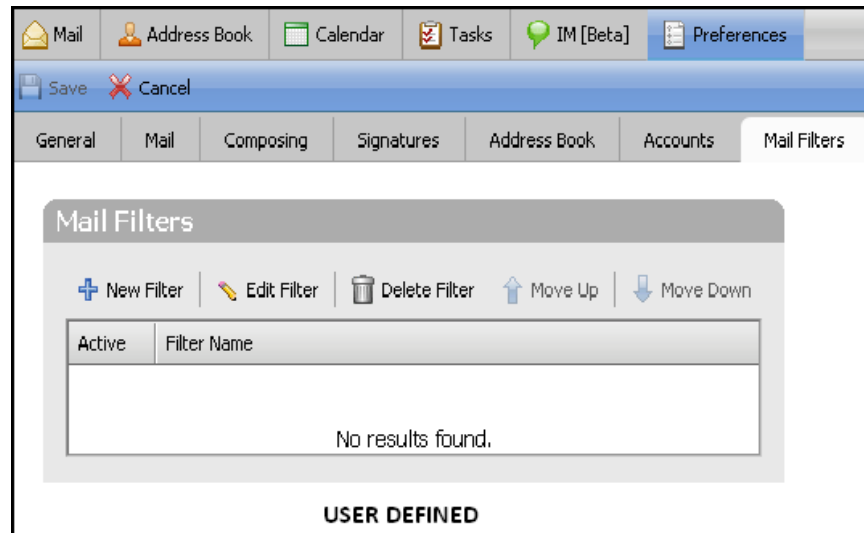
Entourage. . .

1. Click on Message
2. Click on "Junk" icon on Menu bar
3. or
4. Right click and select 'Mark as Junk'

More information:

Remember, filters are a two way system. These can be applied at Drake as well as other mail recipients.

User defined filters are included in most email clients today. With these filters you can forward email to different mailboxes depending on headers or contents. For example, you would put email from each of your friends into a mailbox named after them. You can also use these same filters to forward email to the trash if the origin or contents are suspicious. To do this you need to carefully look at any Spam emails you receive. Try to notice common characteristics, recurring patterns in senders' email addresses, dubious claims in the subject line and so on. You will soon find that Spam filtering using a small number of rules can eliminate a large number of Spam emails. – FOR MORE INFO SEE OUR GETTING STARTED GUIDE on: http://www.drake.edu/it/newservices/Documents/blueview_mail.pdf



Header filters are more sophisticated. They look at the email headers to see if they are forged. Email headers contain information in addition to the recipient, sender and subject fields displayed on your screen. They also contain information regarding the servers that were used in delivering your email (the relay chain). **Many spammers do not want to be traced.** They put false information in the email headers to prevent people from contacting them directly. Some anti spam programs can detect forged headers which are a sure indication that the email is Spam. Not all Spam has forged headers though, so this filter by itself is not sufficient.

Language filters simply filter out any email that is not in your native tongue. It only filters out foreign language Spam, which is not a major problem today, unless the foreign language under question is English. In future, languages other than English are expected to make up an increasingly large percentage of Internet communications. If you do not expect to get emails in another language, this may be a quick and easy way to eliminate some portion of your Spam.

Content filters scan the text of an email and use fuzzy logic to give a weighted opinion as to whether the email is Spam. They can be highly effective, but can also occasionally filter out newsletters and other bulk email that may appear to be Spam. This can usually be overridden by explicitly authorizing email from domains you subscribe to.

Permission filters block all email that does not come from an authorized source. Typically the first time you send an email to a person using a permission filter you will receive an auto-response inviting you to visit a web page and enter some information. Your email then becomes authorized and any future emails you send will be accepted. This is not suitable for all users, but very effective for those that choose to use it, as long as the auto-response email is not blocked by the Spam filter of the initial sender!

What is:

PHISH - In the field of computer security, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication.

SPAM - Spamming is the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. E-mail spam, also known as "bulk e-mail" or "junk e-mail," is a subset of spam that involves nearly identical messages sent to numerous recipients by e-mail. E-mail addresses are collected from chatrooms, websites, newsgroups, and viruses which harvest users' address books, and are sold to other spammers.

419 scam/Advance-fee fraud - An advance fee fraud is a confidence trick in which the target is persuaded to advance sums of money in the hope of realizing a very much larger gain.[1] Among the variations on this type of scam, are the Nigerian Letter (also called the 419 fraud, Nigerian scam, Nigerian bank scam, or Nigerian money offer.