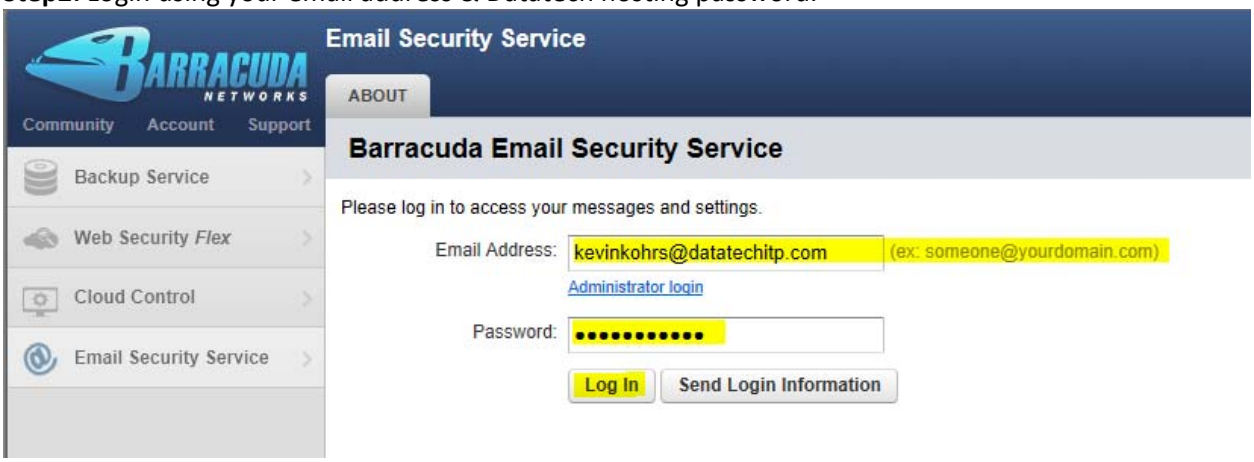
# Barracuda User Guide

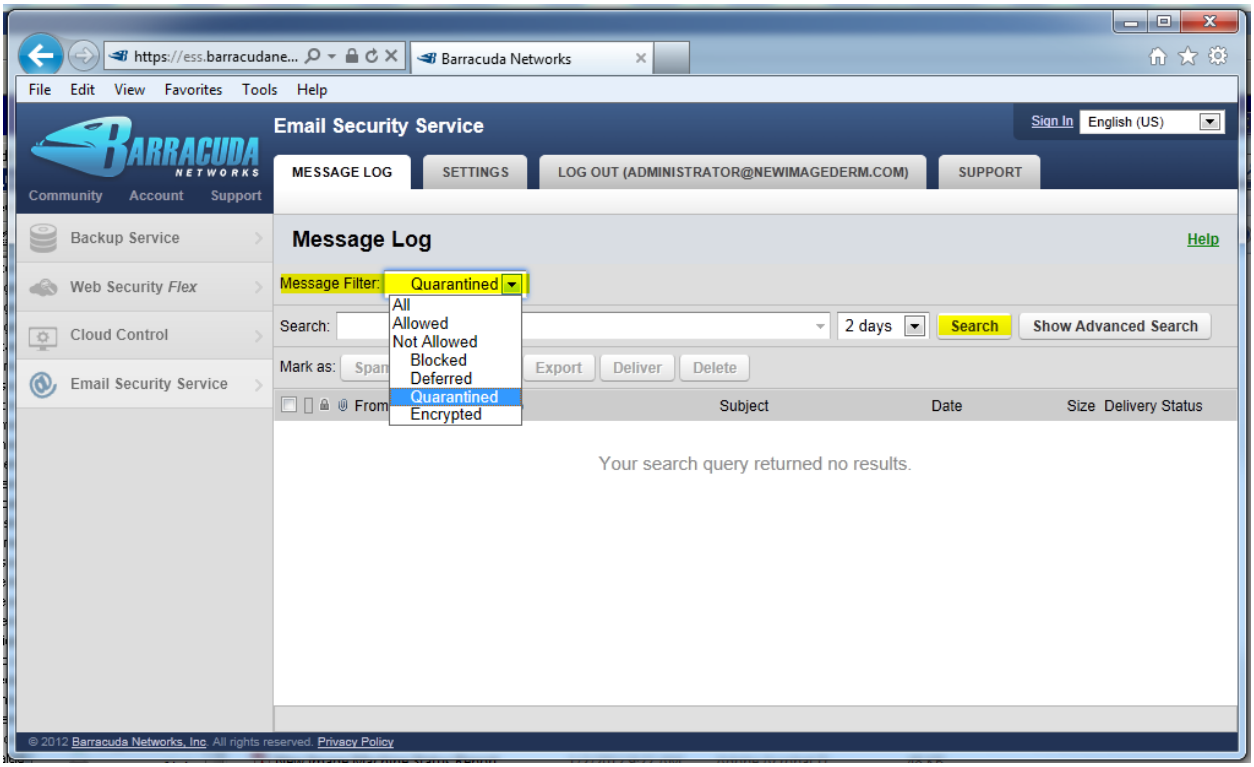
## *Managing your Spam Quarantine*

**Step1:** Open your internet browser and go to [http://myspam.datatechhosting.com](http://myspam.datatechhosting.com) this will automatically redirect you to Barracuda's email security service portal.

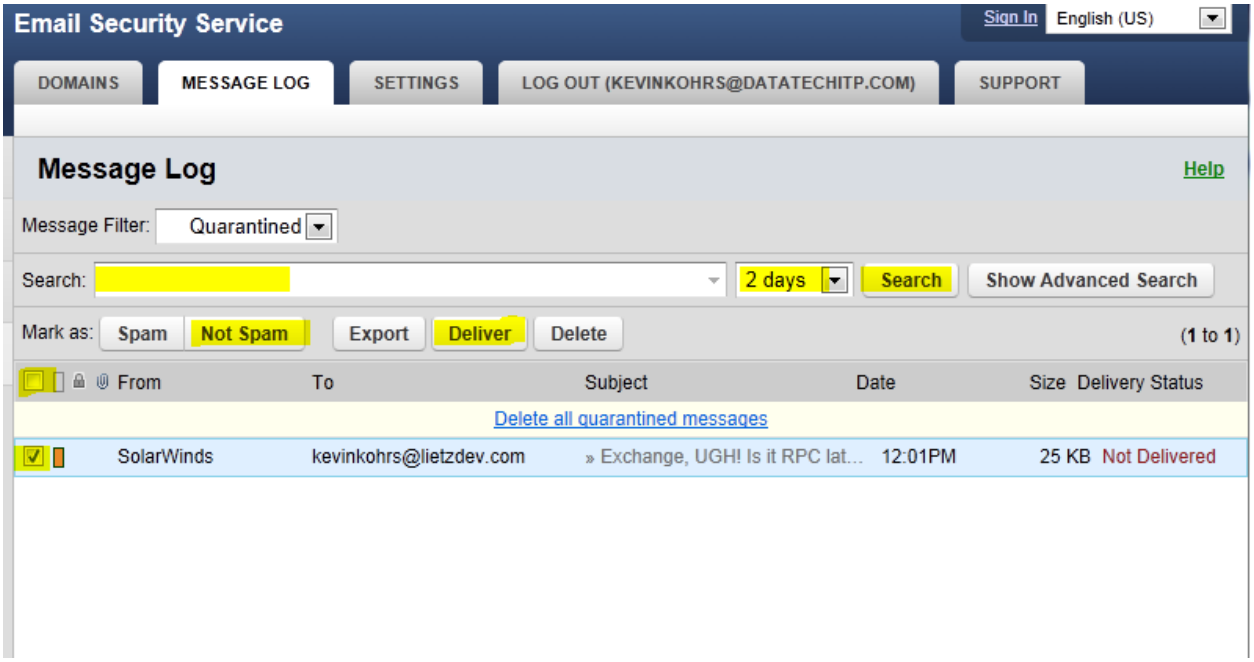
**Step2:** Login using your email address & Datatech hosting password.



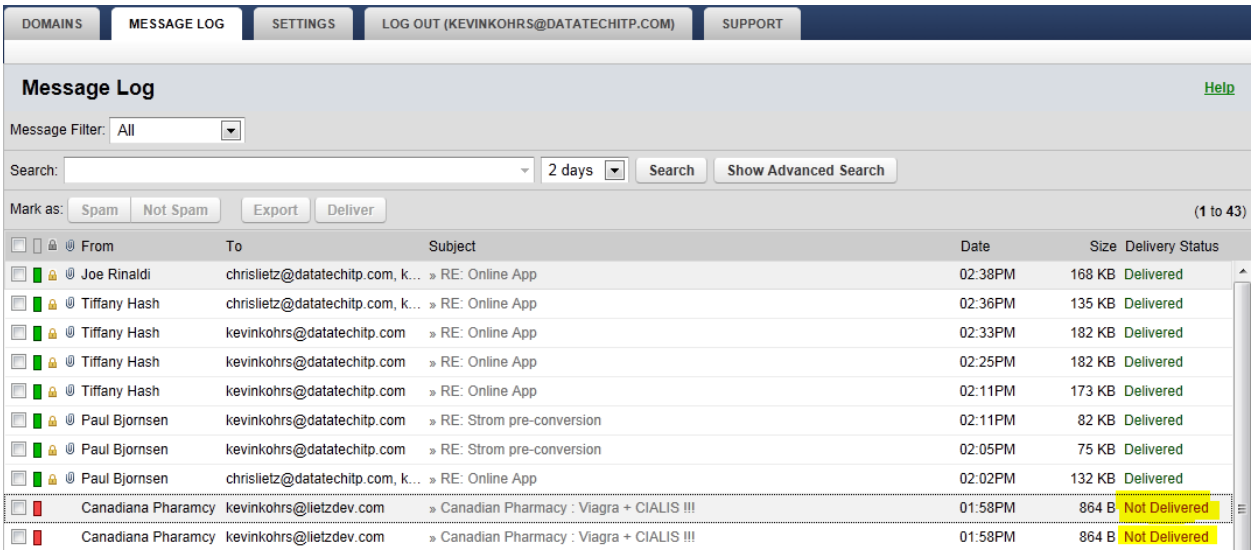

**Step3:** Once you've logged in you will be taken directly to the quarantined message log.



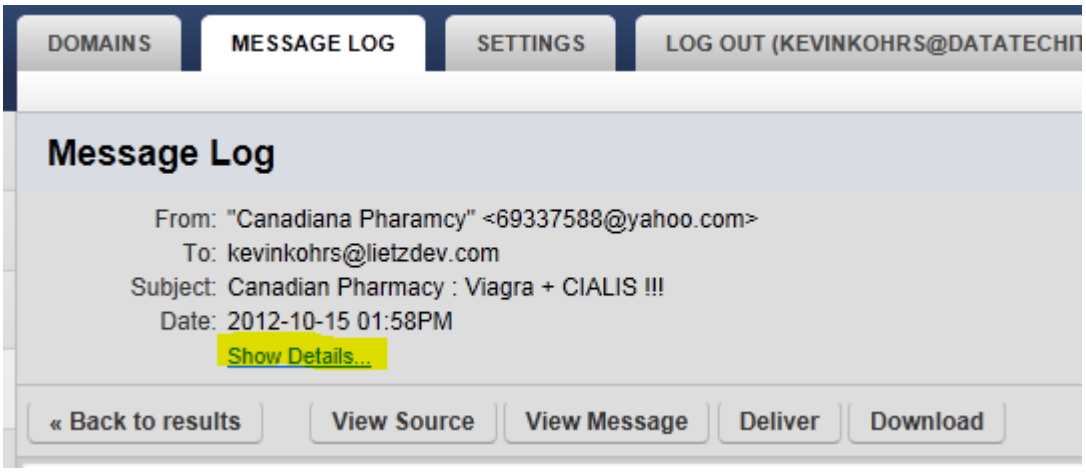
**Step3 cont.:** If you just click on search it will display all messages in the quarantine without any special filters. You can select the individual email you wish to deliver or flag as not spam. If you apply a filter to a specific email and it it brings up several messages you can click on the check box under **mark as** and this will select all mail messages.

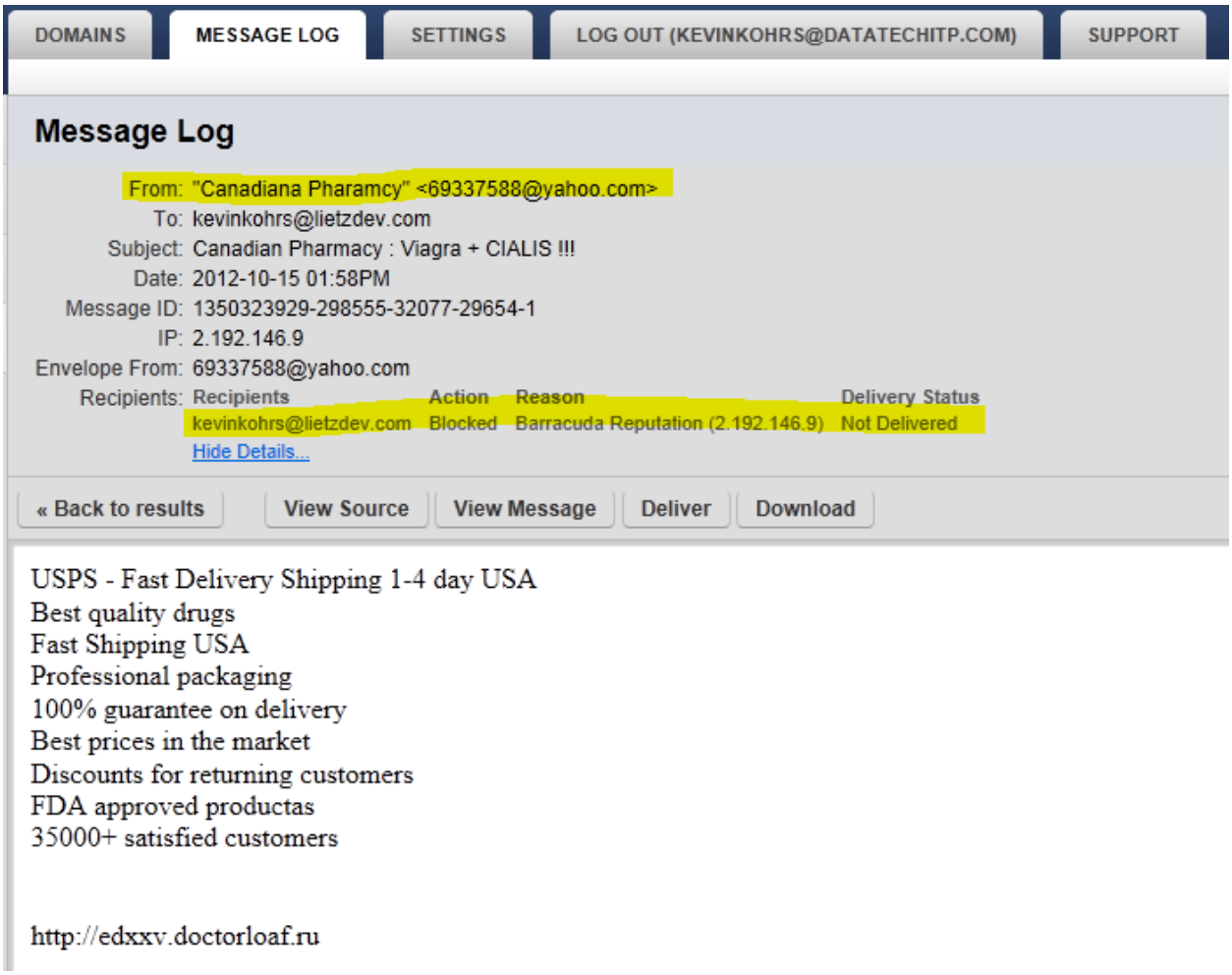



**Step4:** You have the option of adjusting the message filter to include all mail messages and not just quarantined emails. Using this option can allow you to redeliver emails you accidentally deleted or to check delivery status on emails you might not have received.

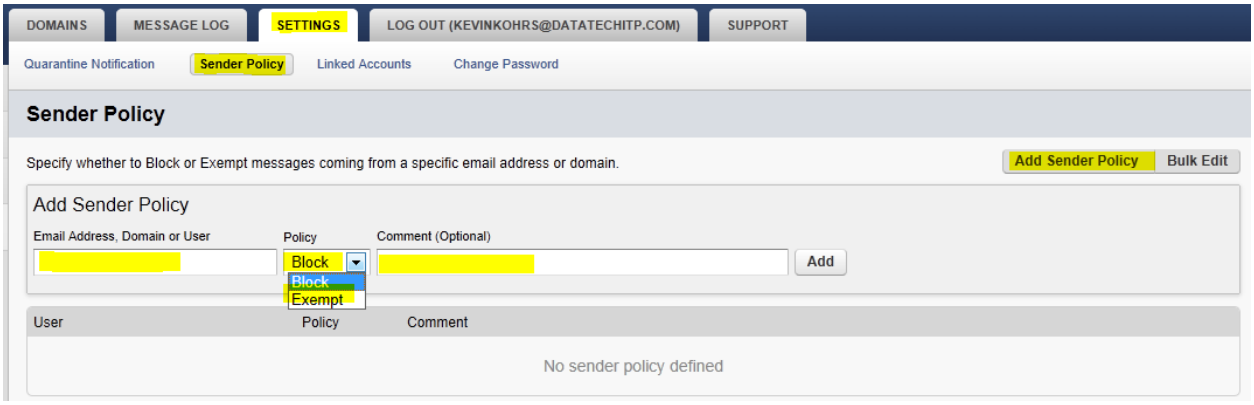


**Step 5:** Once you have opened the message log you will want to click on show details. This will give you detailed information on why a particular email was not delivered. In this particular case because the barracuda reputation filter flagged this email as spam.



**Step6:** To add an email sender exception click on the settings tab and select **Sender Policy** then click **Add Sender Policy**. This will bring up the email address & policy options for you to create an exemption list. Users on this list will be excluded from spam filtering. This should **NOT** be used for emails that are on your domain as it will open you up to spam email attacks. Once you have entered an email address, chosen the policy, and entered a comment click **add**.



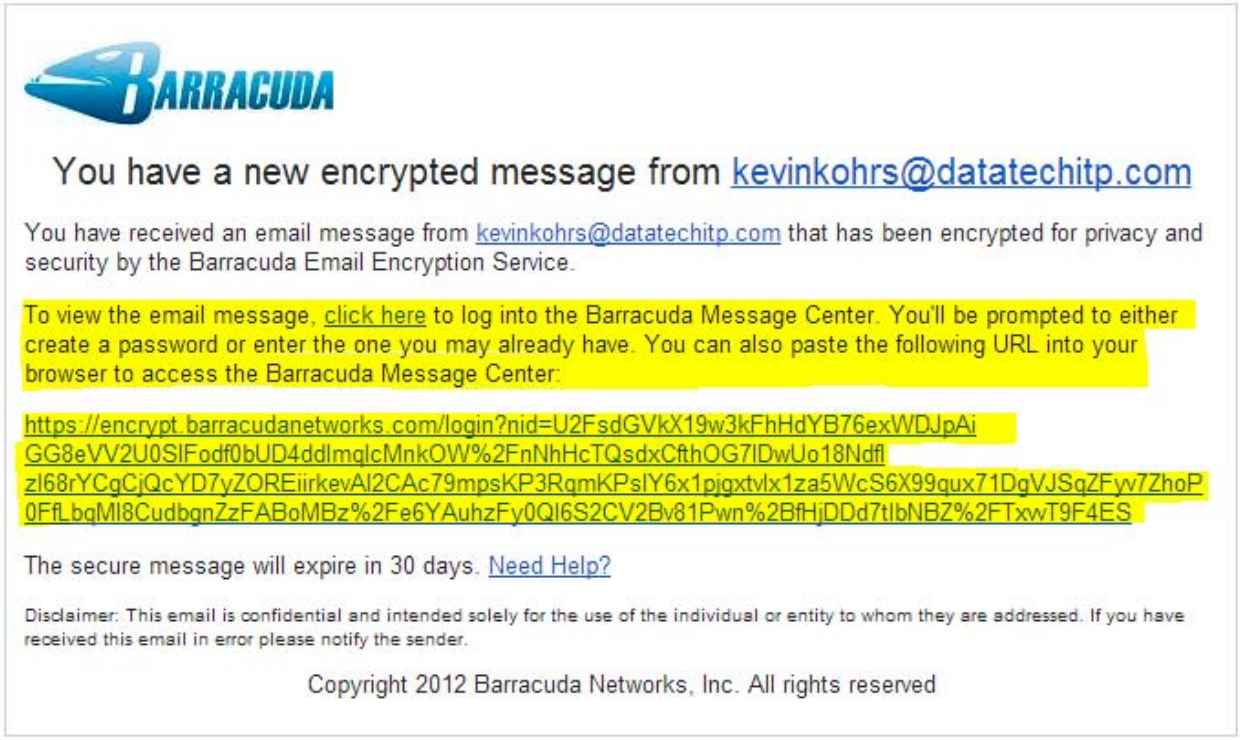

## *Sender Email Encryption Overview*

The email encryption is a fairly seamless integration. Emails you send that contain certain predefined patterns will trigger the encryption automatically. Patterns are highlighted below.

In addition we have added a filter to the subject line. If you type **ENCRYPT** anywhere in the subject it will automatically encrypt the email regardless of content.

## *Recipient Email Encryption Overview*

"What the heck is this"? Might be the first thing you hear from the recipient of an encrypted message. Below is a snapshot of what the recipient receives when you've sent an encrypted message.



BARRACUDA

You have a new encrypted message from kevinkohrs@datatechitp.com

You have received an email message from kevinkohrs@datatechitp.com that has been encrypted for privacy and security by the Barracuda Email Encryption Service.

To view the email message, click here to log into the Barracuda Message Center. You'll be prompted to either create a password or enter the one you may already have. You can also paste the following URL into your browser to access the Barracuda Message Center:

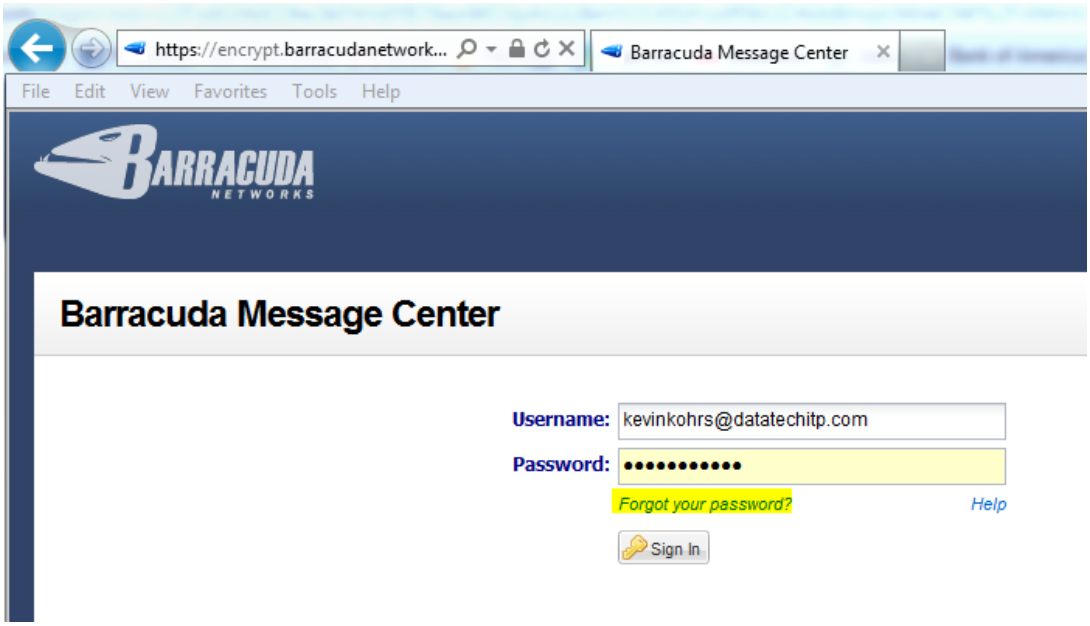
https://encrypt.barracudanetworks.com/login?nid=U2FsdGVkX19w3kFhHdYB76exWDJpAi
GG8eVV2U0SlFodf0bUD4ddlmqlcMnkOW%2FnNhHcTQsdxCfthOG7lDwUo18Ndfl
zl68rYCgCjQcYD7yZOREiirkevAl2CAc79mpsKP3RqmKPslY6x1pjgxtvlx1za5WcS6X99qux71DgVJSqZFyv7ZhoP
0FfLbqMl8CudbgnZzFABoMBz%2Fe6YAuhzFy0QI6S2CV2Bv81Pwn%2BfHjDDd7tlbNBZ%2FTxvT9F4ES

The secure message will expire in 30 days. Need Help?

Disclaimer: This email is confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the sender.

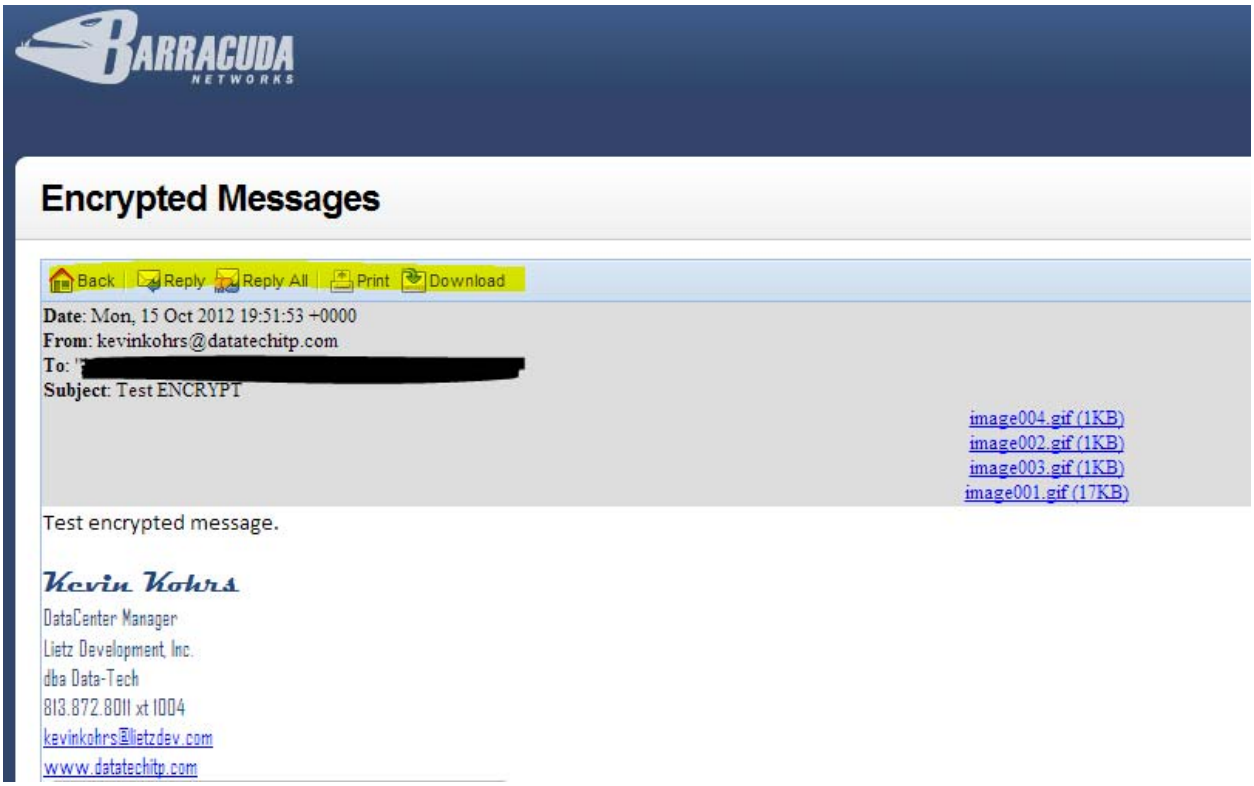
Copyright 2012 Barracuda Networks, Inc. All rights reserved

First time recipients will need to create a password for their email address. Once they have clicked on the **click here** button or the https://encrypt.barracudanetworks.com URL in the message they will be brought to the barracuda message center.

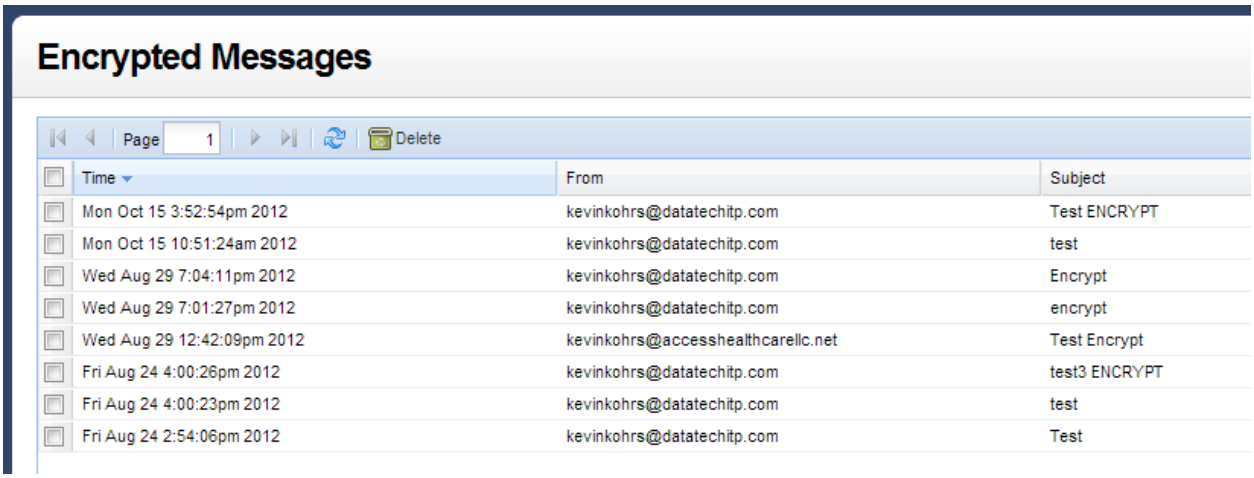


Passwords must contain at least 1 number & a special character. If a user has previously created a password but does not remember they can click on the forgotten password link and it will email them a new password.

Once you have logged in you will be taken to the latest encrypted message. From here on the rest of the emails in the chain will be encrypted and all correspondence will be done via the barracuda message center.




Clicking on the back button at the top of the encrypted message takes you to the inbox of the barracuda message center. Here you will see all messages for your account.




| Time | From | Subject |
|---|---|---|
| Mon Oct 15 3:52:54pm 2012 | kevinkohrs@datatechitp.com | Test ENCRYPT |
| Mon Oct 15 10:51:24am 2012 | kevinkohrs@datatechitp.com | test |
| Wed Aug 29 7:04:11pm 2012 | kevinkohrs@datatechitp.com | Encrypt |
| Wed Aug 29 7:01:27pm 2012 | kevinkohrs@datatechitp.com | encrypt |
| Wed Aug 29 12:42:09pm 2012 | kevinkohrs@accesshealthcarellc.net | Test Encrypt |
| Fri Aug 24 4:00:26pm 2012 | kevinkohrs@datatechitp.com | test3 ENCRYPT |
| Fri Aug 24 4:00:23pm 2012 | kevinkohrs@datatechitp.com | test |
| Fri Aug 24 2:54:06pm 2012 | kevinkohrs@datatechitp.com | Test |

# Barracuda Message Center FAQ

## WHY DID I RECEIVE AN ENCRYPTED MESSAGE?

The sender of the message wanted the contents of the message to be private and secure, so they used the encryption feature of either the Barracuda Spam & Virus Firewall or the Barracuda Email Security Service to encrypt the message. Only you (the intended recipient) will see the message contents when you log into the Barracuda Message Center with a password you create the first time you log in.

## WHAT IS THE BARRACUDA MESSAGE CENTER?

The Barracuda Message Center is a cloud-based email encryption service. The service provides a web-based email client for receiving and replying to encrypted email sent by the Barracuda Spam & Virus Firewall or the Barracuda Email Security Service. The email client looks and behaves much like any web-based email program. Once you log into the Barracuda Message Center, you'll be presented with a list of one or more email messages that were sent to you. All encrypted messages you receive will appear in this list for a finite retention period or until you delete them.

## WHAT ENCRYPTION METHOD WAS USED TO ENCRYPT THE MESSAGE I RECEIVED?

The Barracuda Message Center uses AES-256 bit encryption.

## HOW DO I RETRIEVE AND READ MY ENCRYPTED MESSAGE?

The email notification you received telling you that you received an encrypted email message includes a link to the Barracuda Message Center. The first time you click this link, the Barracuda Message Center will prompt you to create a new password. In the future you can re-use that password to pick up subsequent encrypted messages from the Barracuda Message Center. Once you create a password, you can log in and retrieve your message.

## IF I REPLY TO THE ENCRYPTED MESSAGE, WILL MY REPLY ALSO BE ENCRYPTED?

When you reply to the encrypted email message, the response will also be encrypted and the recipient (who may be the sender of your original encrypted message) will receive a notification, much like the one you received, that includes a link to view and retrieve the message from the Barracuda Message Center. You can address the reply to as many recipients as you like.

## CAN ANYONE ELSE READ THE CONTENTS OF MY ENCRYPTED MESSAGE?

The message can only be viewed when you enter your unique password. It is highly recommended that the password not be shared with anyone else. As long as the password is secure, no one else can read the message.

## HOW LONG ARE MY MESSAGES STORED BY THE BARRACUDA MESSAGE CENTER?

The Barracuda Message Center will store your encrypted email message for 30 days from the date of receipt.

## HOW CAN I SEE THE MESSAGE HEADERS OF ONE OF MY ENCRYPTED EMAILS?

In the Barracuda Message Center, click on the message to open it. Once the message is open, click on the "Show All Headers" link at the upper right of the message.

## HOW DO I GET MY PASSWORD IF I FORGET IT?

On the Login page, click on the "Forgot Password?" link. You'll then be prompted to enter your email address, and the password will be sent to you.

## WHAT CHANGES HAVE THERE BEEN WITH USERNAME CASE-SENSITIVITY?

Previously the Barracuda Message Center created case-sensitive account names. Now all incoming sender and recipient addresses will be not be case-sensitive. If you previously had a mixed case or upper case username you can still login with that username to access your old encrypted messages. All new messages however will be delivered to your lowercased username.

## Predefined Filters for Data Leakage Prevention (DLP)

You can take actions with outbound messages that contain matches to the following pre-made patterns in the subject line, message body or attachment. Select the pattern type, the action (Block, Quarantine or Encrypt) and then check any or all of: **Subject**, **Headers**, **Body** and **Attachment**. The patterns are inserted into the keyword listings and include Credit Card, Social Security, Privacy, and HIPAA formats. To best secure transmission of messages containing this kind of data, select the *Encrypt* action for each type. **Note:** The format of this data varies depending on the country, and these filters are more commonly used in the U.S.; they do not apply to other locales.

- **Credit Cards** - Messages sent through the Barracuda Email Security Service containing recognizable Master Card, Visa, American Express, Diners Club or Discover card numbers will be subject to the action you choose.
- **Social Security** - Messages sent with valid social security numbers will be subject to the action you choose. U.S. Social Security Numbers (SSN) must be entered in the format nnn-nn-nnnn.
- **Privacy** - Messages will be subject to the action you choose if they contain two or more of the following data types, using common U.S. data patterns only: credit cards (including Japanese Credit Bureau), expiration date, date of birth, Social Security number, driver's license number, or phone number. Phone numbers must be entered in the format `nnn-nnn-nnnn` or `(nnn)nnn-nnnn` or `nnn.nnn.nnnn` .
- **HIPAA** - Messages will be subject to the action you choose if they contain TWO of the types of items as described in Privacy above and ONE medical term.

  Because of the millions of ways that any of the above information can be formatted, a determined person will likely be able to find a way to defeat the patterns used above. These filter options are no match for educating employees about what is and is not permissible for transmitting via unencrypted email.