



NEMX Software Corporation

Best Practices Guide

Version 4.2

April, 2004



Chapter 1: Email Policy 3

Benifits of an Email Policy	3
Protection for a Company and its Employees	4
Email User and Administrator Satisfaction	4
Creating an Email Policy	4
Email Policy Content	5
Web References for further information	5
Implementing an Email Policy	5
Add Email Disclaimer	5
Notify Employees	6
Monitoring Email	6

Chapter 2: Monitoring Nemx Power Tools 7

Investigating Filtered Messages	7
Monitoring Performance	9
Examining Quarantined Items	10
Contents of Quarantine mailbox or public folder	11
Contents of a Quarantined Message	12

Chapter 3: False Positives 15

Concept Manager	15
Automatically Friendly Domains	16
Always Friendly Domains	16
Exclude users from Concept Filtering	16
Exclude Originating SMTP Address	17
Spam Manager	18

RBL filtering	19
RBL Policy	19
<i>Free RBLs</i>	20
<i>Subscription Based</i>	20
Weighting	21
Friendly IP Addresses	21
Automatically Friendly Domains	21
Always Friendly Domains	21
Exclude Originating SMTP Address	21
Subject and Header Filtering	22
Always Friendly Domains	22
Exclude Originating SMTP Address	23
Group Exceptions	23

Chapter 4: False Negatives 25

Concept Manager	25
Spam Manager	26
RBL filtering	26
Geographic RBLs	26
Subscription RBLs	27
Header Filtering	27
Ineligible Character Sets	27
Subject Filtering	27
Predetermined Rule Sets	28
Heuristic Pattern Matching	28
Plain Text camouflage	28
<i>Character Substitution</i>	29
<i>Word Hiding</i>	30
Address Filtering	30
Country Domain Filtering	30

Chapter

1

Email Policy

Email is now an important tool for business and personal communication. Since email is such a popular form of communication it is also a potential avenue for employee harassment, confidentiality breaches, legal liability, and lost productivity due to spam. An email policy is the best form of protection for any organization. The following chapter describes:

- Benefits of an Email Policy
- Creating an Email Policy
- Implementing an Email Policy

Benefits of an Email Policy

An email policy describes social and technical methods that benefit a company and its employees. The following describes the benefits of an email policy:

- Protection for a Company and its Employees
- Email User and Administrator Satisfaction

Protection for a Company and its Employees

An email policy outlines acceptable email etiquette to employees and the terms and conditions of email policy violations. The following describes

- protects a corporation which filters email from litigation due to infringements upon employee privacy.
- protects corporation which filters email from litigation due to an unsafe work environment.
- protects a corporation from litigation due to improper use of email facilities by employees.

Email User and Administrator Satisfaction

Users become understandably agitated when important email correspondence is incorrectly filtered as spam. In turn, administrators become agitated when they have to find the important business communication among thousands of quarantined email. An email policy reduces the confusion for employees and email administrators as to why particular emails are filtered. Employees will understand what is considered inappropriate language or intent. Also employees will understand what is considered to be confidential corporate information and potentially harmful file types. The following is a list of benefits of an email policy:

- increased employee satisfaction within a harassment free working environment.
- increased security with an outline of what is considered to be classified content such as sensitive personal, medical or corporate information.
- increased security with an outline of what is considered to be inappropriate file types such as .exe files.
- recovered bandwidth lost to chain letters or personal correspondence with large file attachments

Creating an Email Policy

- Email Policy Content
- Web References for Further Information

Email Policy Content

An email policy outlines the responsibilities and privacy limitations for a company and its employees. The following is a list of items contained within an email policy:

- Inappropriate terms and phrases which constitutes potentially harassing or offensive content.
- Information that is considered to be classified content such as sensitive personal, medical or corporate information.
- File types not considered to be business related such as graphic and executable formats.
- The conditions which constitutes a business related newsletter, forum, newsgroup or chat room.
- The conditions which constitutes monitoring of an employees mailbox

Web References for further information

The following is a list of excellent websites that provide information regarding corporate email policies and email etiquette:

- <http://www.email-policy.com/>
- <http://www.emailreplies.com/>

Implementing an Email Policy

A email policy must be enforced to ensure proper use of corporate email facilities. The following describes email policy implementation:

- Add Email Disclaimers
- Notify Employees
- Monitoring Email

Add Email Disclaimer

Add a disclaimer to all mail referring the recipients of corporate to the corporate email policy. The disclaimer should also include an email address to receive complaints about violations.

Notify Employees

Publish the policy on the corporate intranet site, post printed copies on bulletin boards popular employee and include within terms of employment packages.

Monitoring Email

Apply monitoring as uniformly as possible. It is best not to single out an individual unless there is clear reason to do so. If you single out a person, the company could be found to be discriminating against the individual. Therefore, use monitoring software for all emails on your system.

Chapter

2

Monitoring Nemx Power Tools

Prior to enabling Nemx Power Tools methods for monitoring filtered email need to be understood. Nemx Power Tools monitoring methods reduce administrative interaction and occurrences of incorrectly filtered email (false positives) by identify filtered email quickly and efficiently. The following chapter describes how to monitor Nemx Power Tools

- Investigating Filtered Messages
- Monitoring Performance
- Examining Quarantined Items

Investigating Filtered Messages

Nemx Power Tools administrators that need to quickly locate filtered email search the nmxxsp.log. Nemx Power Tools creates an entry within a file named nmxxsp.log for every filtered email. The following describes how to open the nmxxsp.log

How to open the nmxxsp.log using Notepad.exe.

1. Start | Programs | Accessories | Notepad
2. File | Open
3. Navigate to c:\program files\nemx\nmxxsp and select nmxxsp.log
4. Click Open
5. Disable the menu item Format | Word Wrap

How to search for an email

1. Within Notepad.exe Edit | Find
2. Enter the subject or SMTP address you are searching for example the subject “let me give you some help”.
3. Click OK

The nmxxsp.log file is a comma separated file with columns specifying the details of every filtered email. The following is an example entry of a rule that fired upon an email

```
07/09/2003 - 14:42:35 Content Filter Detection / Message Text  
Violation:  
Rule=viagra, Object=Message Text, Action=Move,  
Mailbox=/O=ExchangeOrganization/OU=ExchangeSite/CN=CONFIGURATION/  
CN=CONNECTI  
ONS/CN=INTERNET MAIL CONNECTOR (EXCHANGESERVER), Folder=<unknown>,  
Subject=Let me give you some help, From=matthew [user@nemx.com],  
Date=Wed,  
Jul 09 2003, 2:41:24 PM, Recip=peter [user@nemx.com]
```

The following chart describes the columns in order as they appear within the nmxxsp.log file.

Column	Description
Component	The component and section the from the previous example the component Content Manager within the Message Body Filtering section.
Rule	Nemx Power Tools rule that triggered upon an email.
Object	Item in the email that caused the Nemx Power Tools rule to trigger.
Action	Nemx Power Tools action that fired after the Nemx Power Tools rule fired.
Mailbox	Mailbox where the email was found within.
Folder Public	Mailbox sub-folder where the message was found within.
Subject	Subject of the email.

Column	Description
From	SMTP address or Exchange user the filtered email originated from.
Date	Date and time the email was filtered.
Recip	Recip SMTP addresses that were to receive the filtered email.

Monitoring Performance

Nemx Power Tools administrators that need to quickly produce reports of filtered email search NEMX_AUDIT_LOG database table. Nemx Power Tools creates a NEMX_AUDIT_LOG table within a specified database through an ODBC connection. The following describes how to configure an Nemx Power Tools for an ODBC connection.

How to Select an ODBC connection.

1. Open the Nemx Power Tools for Exchange configuration
2. Goto the Actions Page
3. Click Add
4. Enable Log Filter History
5. Click Options
6. Select SQL Database
7. Enter the ODBC Connection in the following format <SYSTEM DSN NAME> / u:<sql user> /p:<password>

The following chart describes the information stored within the CSV file and NEMX_AUDIT_LOG table columns:

Column	Description
Date	
Time	
Component	component triggered by filtered email

Column	Description
Category	category set on filtered email
Rule	rule triggered by filtered email
Object	attachment filtered within email
Action Name	action taken on filtered email
Submit Date	
Subject	subject of filtered email
Sender	originator of filtered email
Recipient	recipient of filtered email

Examining Quarantined Items

Possibly harmful, inappropriate or infectious email can be quarantined for later administrative review. The quarantine action holds the original email in a queue and sends a quarantine message to a mailbox or public folder as specified by the Nemx Power Tools Administrator. Within the quarantine message is an embedded copy of the original email. The following describes methods of reviewing quarantined email:

- Contents of a Quarantine mailbox or public folder
- Contents of a Quarantined Message

Contents of Quarantine mailbox or public folder

Each quarantine message that arrives at the quarantine mailbox or public folder contains custom properties. Nemx Power Tools administrators use the custom properties to sort for important information using custom or predefined Outlook Views. The following chart describes each of the custom properties added by Nemx Power Tools:

Display Field	Description
Nemx.Quarantine. Componen	Compent (e.g. Spam Manager) that triggered the quarantine action to fire
Nemx.Quarantine. Rule	Specific rule (e.g. free stuff) that triggered the quarantine action to fire
Nemx.Quarantine. Subject	Subject of the quarantined message
Nemx.Quarantine. Sender	SMTP originator (e.g. support@nemx.com) of the quarantined message
Nemx.Quarantine. SenderDomain	SMTP domain (e.g. nemx.com) of the quarantined message
Nemx.Quarantine. Recips	SMTP recipients (e.g. sales@nemx.com) of the quarantined message

Nemx Power Tools provides predefined Outlook Views to group and sort items by the custom properties. The following chart displays the views with the custom properties that are displayed:

Display Field	By Recipient	By Component	By Domain
Nemx.Quarantine. Component	No	Group By	No
Nemx.Quarantine. Rule	Yes	Yes	Yes
Nemx.Quarantine. Subject	Yes	Yes	Yes

Display Field	By Recipient	By Component	By Domain
Nemx.Quarantine.Sender	Yes	Yes	No
Nemx.Quarantine.SenderDomain	No	No	Group By
Nemx.Quarantine.Recips	Group By	Yes	Yes

Contents of a Quarantined Message

Each quarantine message that arrives at the quarantine mailbox or public folder contains information fields within the message body. The information fields describe the item responsible for triggering a rule within an email. The following is an example of fields added to a quarantine message:

```
Component = Spam Filter Detection
Category = Subject Violation
Rule = free stuff
Object = Subject
Action = Test - New Concept Manager
```

```
Mailbox = Windows 2000 Default SMTP Server
Folder = Unknown
Recips = smtp:sales@nemx.com
```

The following chart describes the fields present within the body of a quarantine message:

Field	Description
Component	Component (e.g. Spam Manager) that triggered the quarantine action.
Category	Rule Category (e.g. Subject Violation) that triggered the quarantine action.
Rule	Specific rule (e.g. free stuff) that triggered the quarantine action.
Object	Item that caused the rule to trigger.
Action	Name of the action triggered by a rule.

Examining Quarantined Items

Field	Description
Mailbox	Mailbox that triggered the quarantine action. (Windows 2000 Default SMTP Server or Internet Mail Service indicates mailed blocked going to or arriving from the Internet)
Folder	Mailbox folder (e.g. inbox) of the email that triggered the quarantine action. NOTE only applies to internal email. (Not applicable to mail arriving from or going to the Internet)
Recipient	SMTP recipients (e.g. sales@nemx.com) of the quarantined message

Chapter

3

False Positives

Emails incorrectly identified as spam are a liability to an organization relying upon email for business correspondence. Email incorrectly identified as spam are considered to be false positives. False positives that are placed in the quarantine folder requires time and effort to find. To reduce the number of false positives, Nemx Power Tools allows for adjustments within the following components.

- Concept Manager
- Spam Manager
- Group Exceptions

Concept Manager

This section describes the best way to prevent false positives within Concept filtering using the following methods.

- Automatically Friendly Domains
- Always Friendly Domains
- Exclude users from Concept Filtering
- Exclude Originating SMTP Address

Automatically Friendly Domains

To reduce the occurrence of false positives Friendly Domains automatically track the frequency of all email heading outbound from the Exchange Server to external domains for example nemx.com. Specific domains with frequently email delivery are considered to be a trusted relationship and are excluded from spam filtering. For more information reference the Operations Manager in the chapter Friendly Domains under the section Automatic List.

Always Friendly Domains

A customer or supplier may be considered a trusted domain, known not to send spam. To ensure email from trusted domains always arrive unfiltered create an Always Friendly Domain to bypass the Nemx Power Tools filtering. Always Friendly Domains operates upon the FROM field within the header of an inbound email passing inbound from the internet. An email is considered to be from a Friendly Domain if the FROM field domain matches an item on the Always Friendly list. For more information reference the Operations Manager in the chapter Friendly Domains under the section Always Friendly.

Exclude users from Concept Filtering

To reduce the number of false positives, Nemx Power Tools permits groups of users that do not wish to have email filtered by Concept Manager.

Within Exchange Server create a distribution list with the members excluded from Nemx Power Tools filtering.

Create an Action to respond to "Do Nothing".

1. Open the Nemx Power Tools configuration
2. On the Actions tab select Spam and Contents
3. Click Ok
4. In the Action Name field type Do Nothing
5. Click Ok

Create a Rule to catch all mail destined to the distribution list members

1. Open the Nemx Power Tools configuration
2. On the Content Manager tab in the Message Body Filtering section click Rules
3. Enable the Active field
4. In the Rule field type *
5. Select in the Action field Do Nothing
6. Enable the fields Inbound and Outbound in the Transfer Mode section (for Internet email)
7. Select Halt Filtering on Message in the Behavior section
8. Select Include in the Restrictions field
9. Click Add/Remove and select the <exempt distribution list>
10. Click Ok

Exclude Originating SMTP Address

An SMTP address may be considered a trusted address, known not to send spam. To ensure email from trusted addresses always arrive unfiltered create the following.

Mark the Originator Address to bypass the RBL filtering

1. Open the Nemx Power Tools for Exchange configuration
2. Select the Action Tab
3. Select "Spam and Content Actions" in the Action Type section
4. Click Add
5. Enter "Do Nothing" in the Action Name field
6. Click Ok
7. Goto the Spam Manager Tab
8. Click Addresses in the Originator Filtering section
9. Click Add
10. Check Active
11. Enter address of originator in the Address field
12. Select the action "Do Nothing"
13. Select "Halt filtering on Message in the Behavior section
14. Check "Inbound" in the Transfer Mode section
15. Click Ok
16. Click Ok
17. Click Apply

Spam Manager

This section describes the best way to prevent false positives within Spam Manager within the following filters.

- RBL Filtering
- Subject and Header Filtering

RBL filtering

This section describes the best way to prevent false positives within RBL filtering using the following methods.

- RBL Policy
- Weighting
- Friendly IP Addresses
- Automatically Friendly Domains
- Always Friendly Domains
- Excluding Originating SMTP Address

RBL Policy

RBLs have different policies detailing how an SMTP server qualifies as a spam relay host. Because each policy may not match your requirements exactly, certain RBLs may not produce accurate results

RBL policies based upon unconfirmed reports and automated testing are considered to be aggressive. Large Internet Service Providers (ISPs) are often included on RBLs that have aggressive policies. Policies based solely on confirmed reports will block less spam; however, they will trigger fewer false positives during filtering. Ensure the policy matches your corporate policy of what is considered a spam relay host. The following describes the different RBL options.

- free RBLs
- subscription based RBLs

Free RBLs

Free and subscription-based RBLs are available on the Web. Free RBL servers, such as <http://www.spamcop.net> and <http://www.dsbl.org>, are available to everyone at no cost. During times of high email traffic on the Internet, free RBL servers become very busy and will slow down or even fail to respond to DNS queries. The following chart describes the policies of a few RBLs

RBL	Website	Description
unconfirmed.dsbl.org	www.dsbl.org	Unconfirmed reports from spam recipients
list.dsbl.org	www.dsbl.org	Confirmed reports from spam recipients
relays.ordb.org	www.ordb.org	Automated testing of SMTP server for open relay capabilities
	www.blackholes.us	IP ranges of country's suspected of sending spam
bl.spamcop.org	www.spamcop.org	Spam trap reports generated by mailboxes which have never sent an outbound message
rfc.ignorant.org	www.rfc-ignorant.org	Non-rfc compliant SMTP servers

Subscription Based

Subscription-based RBL servers, such as <http://www.mail-abuse.org/>, <http://www.postfixgate.com/>, and <http://www.maildeflector.net/> are available to subscribers. DNS transfers from the RBL server to the paying customer's local DNS server are available. RBL queries are then made to the local DNS server removing the dependance upon public RBL servers and internet bandwidth.

Weighting

Aggressive approaches, such as automated testing and countries suspected of sending, may give an unsatisfactory level of false positives. However, aggressive approaches do give clues to potential spam relay hosts. If enough of the clues occur, then it is desirable to filter a message as spam. A simple weighting procedure with three defined weight levels of "reliable", "potential", and "unconfirmed" is invaluable for reducing the number of false positives. For more information reference the Operations Manager in the chapter Spam Manager under the section RBL Database Rules | RBL weighting.

Friendly IP Addresses

Legitimate customers may have unsecured SMTP servers that are relaying spam from a third party. Notify the customer's email administrator and add the problem server as a temporary Friendly IP. IP addresses listed as friendly will bypass the RBL filter. For more information reference the Operations Manager in the chapter Spam Manager under the section RBL Database Rules | Adding Friendly IP Addresses.

Automatically Friendly Domains

To reduce the occurrence of false positives Friendly Domains automatically track the frequency of all email heading outbound from the Exchange Server to external domains for example nemx.com. Specific domains with frequent email delivery are considered to be a trusted relationship and are excluded from spam filtering. For more information reference the Operations Manager in the chapter Friendly Domains under the section Automatic List.

Always Friendly Domains

A customer or supplier may be considered a relay host by other institutions including RBLs. When an RBL contains a trusted domain, known not to send spam, create an Always Friendly Domain to bypass the Nemx Power Tools filtering. Always Friendly Domains operates upon the FROM field within the header of an inbound email passing inbound from the internet. An email is considered to be from a Friendly Domain if the FROM field domain matches an item on the Always Friendly list. For more information reference the Operations Manager in the chapter Friendly Domains under the section Always Friendly.

Exclude Originating SMTP Address

An SMTP address may be considered a trusted address, known not to send spam. To ensure email from trusted addresses always arrive unfiltered create the following.

Mark the Originator Address to bypass the RBL filtering

1. Open the Nemx Power Tools for Exchange configuration
2. Select the Action Tab
3. Select "Spam and Content Actions" in the Action Type section
4. Click Add
5. Enter "Do Nothing" in the Action Name field
6. Click Ok
7. Goto the Spam Manager Tab
8. Click Addresses in the Originator Filtering section
9. Click Add
10. Check Active
11. Enter address of originator in the Address field
12. Select the action "Do Nothing"
13. Select "Halt filtering on Message in the Behavior section
14. Check "Inbound" in the Transfer Mode section
15. Click Ok
16. Click Ok
17. Click Apply

Subject and Header Filtering

The following two options can be used to bypass the subject and header filtering.

- Always Friendly Domains
- Exclude Originating SMTP Address

Always Friendly Domains

A customer or supplier may be considered a trusted domain, known not to send spam. To ensure email from trusted domains always arrive unfiltered create an Always Friendly Domain to bypass the Nemx Power Tools filtering. Always Friendly Domains operates upon the FROM field within the header of an inbound email passing inbound from the internet. An email is considered to be from a Friendly Domain if the FROM field domain matches an item on the Always Friendly list. For more information reference the Operations Manager in the chapter Friendly Domains under the section Always Friendly.

Exclude Originating SMTP Address

An SMTP address may be considered a trusted address, known not to send spam. To ensure email from trusted addresses always arrive unfiltered create the following.

Mark the Originator Address to bypass the header filtering

1. Open the Nemx Power Tools for Exchange configuration
2. Select the Action Tab
3. Select "Spam and Content Actions" in the Action Type section
4. Click Add
5. Enter "Do Nothing" in the Action Name field
6. Click Ok
7. Goto the Spam Manager Tab
8. Click Addresses in the Originator Filtering section
9. Click Add
10. Check Active
11. Enter address of originator in the Address field
12. Select the action "Do Nothing"
13. Select "Halt filtering on Message in the Behavior section
14. Check "Inbound" in the Transfer Mode section
15. Click Ok
16. Click Ok
17. Click Apply

Group Exceptions

Certain rules may only apply to certain departments or groups of people. For example, rules applied to administrators would not be the same as rules applied to students. Distribution lists can be included or excluded from a Address, Subject, Header, Message Body, Attachment and Concept filtering as described below.

Within Exchange Server create a distribution list with the members excluded from Nemx Power Tools filtering.

Create an Action to respond to "Do Nothing".

1. Open the Nemx Power Tools configuration
2. On the Actions tab select Spam and Contents
3. Click Ok
4. In the Action Name field type Do Nothing
5. Click Ok

Create a Rule to catch all mail destined to the distribution list members

1. Open the Nemx Power Tools configuration
2. On the Spam Manager tab click Addresses
3. Enable the Active field
4. In the Address field type *
5. Select in the Action field Do Nothing
6. Enable the fields Inbound and Outbound in the Transfer Mode section (for Internet email)
7. Select Halt Filtering on Message in the Behavior section
8. Select Include in the Restrictions field
9. Click Add/Remove and select the <exempt distribution list>
10. Click Ok

Chapter

4

False Negatives

Filtering email requires finding patterns that distinguish spam from business email. Patterns must match the greatest set of spam as defined by your email policy while matching only the smallest set of business email. Email incorrectly identified as legitimate mail are considered false negatives. This chapter includes information about reducing false negatives for the following components

- Spam Manager
- Content Manager
- Concept Manager

Concept Manager

Concept Manager provides intelligent filtering for anti-spam and content protection. Typically spam with profane or obscene terminology is effectively caught using simple key word searches. Pornography with embedded images, or spam with general mass marketing concepts, pass through undetected by simple text searches. By detecting the meaning of an email, Concept Manager detects and filters inappropriate or spam concepts. The following describes how to submit any email missed by Concept Manager:

How to send sample Spam emails

1. Open Outlook.
2. Select the menu Action | New Message.
3. In the "To:" field type analysis@nemx.com.
4. Drag a message from a folder into new the message.
5. In "To:" field right click on analysis@nemx.com and select the menu item Properties.
6. Enable the item "Always send to this recipient in Microsoft Outlook rich-text".

Spam Manager

This section describes the best way to prevent false positives within Spam Manager using the following methods

- RBL filtering
- Address filtering
- Header filtering
- Subject filtering

RBL filtering

Spam relay hosts are SMTP servers that either originate spam email or relay spam. A Real-Time Blackhole List (RBL) is a Domain Name Server (DNS) server which contains the IP addresses of SMTP servers considered to be spam relay hosts. For further information about RBL filtering refer to the Operations Manual within the chapter Spam Manager under the section RBL Database Rules. The following section describes methods for improving RBL Filtering:

- Geographic RBLs
- Subscription RBLs

Geographic RBLs

All countries do not currently have legislation for distribution of spam. Spam travels through SMTP servers within countries without spam legislation to prevent possible. For organizations that only receive domestic business correspondence it is possible to filter email based upon the geographical location of the originating SMTP server. To reduce administrative costs Nemx Software provides predetermined rule sets for Geographic RBLs.

Subscription RBLs

Subscription-based RBL servers, such as <http://www.mail-abuse.org/>, <http://www.postfixgate.com/>, and <http://www.maildeflector.net/> are available to subscribers. DNS transfers from the RBL server to the paying customer's local DNS server are available. RBL queries are then made to the local DNS server removing the dependence on public RBL servers and internet bandwidth.

Header Filtering

Header rules operate on the header of email traveling inbound through the Internet Mail Service. The following section describes methods for improving Header Filtering:

- Ineligible Character Sets

Ineligible Character Sets

Filtering email based on the foreign character sets increases the accuracy of header filtering rules. Text in foreign character sets may not be legible to employees within your organization, and can therefore be considered unimportant or unnecessary. To reduce administrative costs Nemx Software provides predetermined rule sets for all possible character sets.

Subject Filtering

The first and most common method of filtering email is based upon selected key words and phrases in either the subject line or text of the message, including such “sound the alarms” terms as Mortgage, Credit, \$\$\$ or any of a number of pornographic references. The following section describes methods to optimize filtering based upon key words and phrases.

- Predetermined Rule Sets
- Heuristic Pattern Matching

Predetermined Rule Sets

While highly useful as a first line of defense, it is important to reduce administrative costs with predetermined rule sets from Nemx Software as follows

- pornographic
- mediacaal
- pharماسutical
- financial
- racial slurs

Heuristic Pattern Matching

In general, most email filtering, (or secure content management), solutions provide subject and message body filtering. Spammers have responded by disguising their phrases, such as turning “exciting mortgage offer” into “exciting!!!mortgage!!!offer”. Nemx Power Tools subject filtering offers the capability to select a Heuristic level for more accurate pattern detection. This section describes how Heuristic levels filter camouflaged email:

- Plain Text camouflage

Plain Text camouflage

Plain text camouflage is used to hide pornographic and spam patterns from simple plain text searches. Plain text camouflage is dependant upon human pattern recognition to translate intentional typos (e.g. Viägrä_At_Its_Lowest_Pricés_Evèr!) into a meaningful statement (e. g. Viagra at its lowest prices ever!). The two methods of plain text camouflage character substitution and word hiding are described in this section as follows:

- Character Substitution
- Word Hiding

Character Substitution

Simple text searches look for specific patterns such as viagra within the subject or message body of an email. Spam attempts to bypass these filters by substituting characters with close relatives (e.g. viägrä). Heuristics intelligently adjust the search pattern to detect the close character relatives to accurately find the desired pattern.

Intended Character	Substituted Character
1	1
i	l iïîı
o	o0òóôõö
a	@áâãäå\$
u	ùúûüμ
e	èéêë
n	ñ
y	ÿ
c	ç
b	β
s	\$

Word Hiding

Simple text searches look for specific patterns such as "viagra at its lowest price" within the subject or message body of an email. Spam attempts to bypass these filters by substituting space characters with close relatives (e.g. viagara_at_its_lowest_price) and by adding more character spaces (e.g. viagara at its lowest price). Heuristics intelligently adjust the search pattern to detect the close character relatives and added character spaces to accurately find the desired pattern.:

Heuristic Level	Definition
None	pattern ex (easy money)
Low	pattern separated by any number of spaces will be caught. ex (easy money)
Medium	pattern separated by any character other than an alpha or numeric will be caught. ex (easy_money)
High	pattern separated by any character other than an alpha will be caught. ex (easy111money)

Address Filtering

Address filtering operates on the From field for email traveling inbound through the Internet Mail Service and operates on the To field for email traveling outbound through the Internet Mail Service. For further information about Address filtering refer to the Operations Manual within the chapter Spam Manager under the section Address Rules.

Country Domain Filtering

Filtering email by means of country domain for inbound messages is reliable since email originating from certain countries may not be associated with your organization. Nemx Power Tools includes a predetermined rule sets to reduce administrative costs. The following is a list of all country domains that are included with the predetermined rule sets.

Domain	Country
AD	Andorra
AE	United Arab Emirates
AF	Afghanistan

Domain	Country
AG	Antigua and Barbuda
AI	Anguilla
AL	Albania
AM	Armenia
AN	Netherlands Antillies
AO	Angola
AQ	Antartica
AR	Argentina
AS	American Samoa
AT	Austria
AU	Australia
AW	Aruba
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BD	Bangladesh
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BI	Burundi
BJ	Benin
BM	Bermuda
BN	Brunei Darussalam
BO	Bolivia
BR	Brazil

Domain	Country
BS	Bahamas
BT	Bhutan
BV	Bouvet Island
BW	Botswana
BY	Belarus
BZ	Belize
CA	Canada
CC	Cocos (Keeling) Islands
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Cote D'Ivoire (Ivory Coast)
CK	Cook Islands
CL	Chile
CM	Cameroon
CN	China
CO	Columbia
CR	Costa Rica
CS	Czechoslovakia (former)
CU	Cuba
CV	Cape Verde
CX	Christmas Island
CY	Cyprus
CZ	Czech Republic
DE	Germany

Domain	Country
DJ	Djibouti
DK	Denmark
DM	Dominica
DO	Dominican Republic
DZ	Algeria
EC	Ecuador
EE	Estonia
EG	Egypt
EH	Western Sahara
ER	Eritrea
ES	Spain
ET	Ethiopia
FI	Finland
FJ	Fiji
FK	Falkland Islands (Malvinas)
FM	Micronesia
FO	Faroe Islands
FR	France
FX	France, Metropolitan
GA	Gabon
GB	Great Britain (UK)
GD	Grenada
GE	Georgia
GF	French Guiana
GH	Ghana

Domain	Country
GI	Gibraltar
GL	Greenland
GM	Gambia
GN	Guinea
GP	Guadeloupe
GQ	Equatorial Guinea
GR	Greece
GS	S. Georgia and S. Sandwich Isls.
GT	Guatemala
GU	Guam
GW	Guinea-Bissau
GY	Guyana
HK	Hong Kong
HM	Heard and McDonald Islands
HN	Honduras
HR	Croatia (Hrvatska)
HT	Haiti
HU	Hungary
ID	Indonesia
IE	Ireland
IL	Israel
IN	India
IO	British Indian Ocean Territory
IQ	Iraq
IR	Iran

Domain	Country
IS	Iceland
IT	Italy
JM	Jamacia
JO	Jordan
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KH	Cambodia
KI	Kiribati
KM	Comoros
KN	Saint Kitts and Nevis
KP	Korea (North)
KR	Korea (South)
KW	Kuwait
KY	Cayman Islands
KZ	Kazakhstan
LA	Laos
LB	Lebanon
LC	Saint Lucia
LI	Liechtenstein
LK	Sir Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg

Domain	Country
LV	Latvia
LY	Libya
MA	Morocco
MC	Monaco
MD	Moldova
MG	Madagascar
MH	Marshall Islands
MK	Macedonia
ML	Mali
MM	Myanmar
MN	Mongolia
MO	Macau
MP	Northern Mariana Islands
MQ	Martinique
MR	Mauritania
MS	Montserrat
MT	Malta
MU	Mauritius
MV	Maldives
MW	Malawi
MX	Mexico
MY	Malaysia
MZ	Mozambique
NA	Namibia
NC	New Caledonia

Domain	Country
NE	Niger
NF	Norfolk Island
NG	Nigeria
NI	Nicaragua
NL	Netherlands
NO	Norway
NP	Nepal
NR	Nauru
NT	Neutral Zone
NU	Niue
NZ	New Zealand (Aotearoa)
OM	Oman
PA	Panama
PE	Peru
PF	French Polynesia
PG	Papua New Guinea
PH	Philippines
PK	Pakistan
PL	Poland
PM	St. Pierre and Miquelon
PN	Pitcairn
PR	Puerto Rico
PT	Portugal
PW	Palau
PY	Paraguay

Domain	Country
QA	Qatar
RE	Reunion
RO	Romania
RU	Russian Federation
RW	Rwanda
SA	Saudi Arabia
Sb	Solomon Islands
SC	Seychelles
SD	Sudan
SE	Sweden
SG	Singapore
SH	St. Helena
SI	Slovenia
SJ	Svalbard and Jan Mayen Islands
SK	Slovak Republic
SL	Sierra Leone
SM	San Marino
SN	Senegal
SO	Somalia
SR	Suriname
ST	Sao Tome and Principe
SU	USSR (former)
SV	El Salvador
SY	Syria
SZ	Swaziland

Domain	Country
TC	Turks and Caicos Islands
TD	Chad
TF	French Southern Territories
TG	Togo
TH	Thailand
TJ	Tajikistan
TK	Tokelau
TM	Turkmenistan
TN	Tunisia
TO	Tonga
TP	East Timor
TR	Turkey
TT	Trinidad and Tobago
TV	Tuvalu
TW	Taiwan
TZ	Tanzania
UA	Ukraine
UG	Uganda
UK	United Kingdom
UM	US Minor Outlying Islands
US	United States
UY	Uruguay
UZ	Uzbekistan
VA	Vatican City State (Holy See)
VC	Saint Vincent and the Grenadines

Domain	Country
VE	Venezuela
VG	Virgin Islands (British)
VI	Virgin Islands (U.S.)
VN	Viet Nam
VU	Vanuatu
WF	Wallis and Futuna Islands
WS	Samoa
YE	Yemen
YT	Mayotte
YU	Yugoslavia
ZA	South Africa
ZM	Zambia
ZR	Zaire
ZW	Zimbabwe
COM	US Commercial
EDU	US Educational
GOV	US Government
INT	International
MIL	US Military
NET	Network
ORG	Non-Profit Organization
ARPA	Old style Arpanet
NATO	Nato field