The Wayback Machine - https://web.archive.org/web/20090202193636/http://www.lashback.com:80/ToolbarDownload.aspx

lashback™

You can have the power of LashBack's Safe Unsubscribe technology. This **FREE** toolbar will unsubsribe you from unwanted junk email from right inside your favorite email application.



Basic Toolbar - FREE Forever!
If you're happy with your current spam filter, keep it! LashBack: Basic works with any spam filter by adding our unsubscribe toolbar to your email client.

Basic Toolbar

Advanced Toolbar - FREE Forever!
Our Basic program, plus junk mail filtering! Automatically identify and remove spam from your inbox and safely unsubscribe from spam.

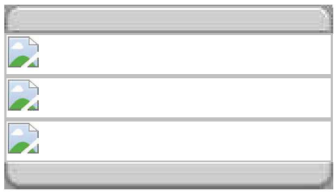
Advanced Toolbar

© 2003-2009 LashBack, LLC., 555 Washington Ave. Suite 400, St. Louis, MO 63101

MICROSOFT CORP.
EXHIBIT 1006

The Wayback Machine - https://web.archive.org/web/20090213235949/http://www.lashback.com:80/support/ToolbarFAQ.aspx





Feature Comparison Chart

Outlook Toolbar FAQ

Quick Links

About Spam and How to Fight It
How LashBack Works
Setup, Cost and Upgrades
Technical Questions

About Spam and How to Fight It

What is 'Spam' and how does it affect me?

Depending on who you ask, 'Spam' could be defined in dozens of ways. However, the average consumer defines Spam as "unwanted email." This is the definition we've adopted.

Spam is annoying, can lower productivity, threaten the security of your computer and even deliver objectionable or offensive content to your email inbox.

What are my options in dealing with Spam? Which is the best?

While most of the world is simply trying to ignore spam with the "delete" key, others have recognized that spam is becoming unmanageable and grows in quantity the longer you use an email address. Many fight spam with:

- **Blocking** – Your email program or ISP (Internet Service Provider) may allow you to Block specific senders from delivering any email to you. This allows you to block regular senders of spam. Unfortunately, since spammers constantly change the addresses they send from this method only stops the least sophisticated spammers and hardly any spam.
- **Filters** – Your ISP, email provider or private software company can sometimes provide a filtering technology that attempts to identify spam (by keywords) before it arrives in your inbox and diverts that message into a "Junk Mail" or "Spam" folder, where it is later deleted. The problem with this method is that 'good' email is often identified as spam and deleted without your knowledge. These are called "false positives" and are the biggest problem with what would otherwise be the most effective way to combat spam.
- **Opting Out (Unsubscribing)** – Many commercial emails provide a button or link that you can click to Opt-Out of the sender's mailing list so you don't get any messages from that sender in the future. The US government has recently identified this as the best way for its citizens to determine which email they choose to receive and which they choose not to receive. The biggest drawback to this method is that (as of December 2003) some commercial emails either do not have opt-out mechanisms or do not have ones that work. Recent legislation (the CAN-SPAM Act) seeks to ensure that ALL commercial email in the future have working unsubscribe functions. Based on this development, Opting Out will be the best long-term solution to spam.

Which methods does LashBack use to fight against Spam?

LashBack incorporates nearly all of the modern methods in spam-fighting. It gives the option to Block specific senders, allows you to filter future messages based on the information that LashBack members supply, and will allow you to opt-out of spam with the click of a button.

If 'opting-out' of spam is the best long-term solution to spam, why do you also bother to block and filter spam?

We at LashBack know that Opting Out will ultimately result in the least Spam received by its members, but also recognize that Blocking and Filtering can bring a more immediate result to spam-elimination and provide some personal customization that many email users desire. By using all three popular methods (and more), we can ensure that our customers receive the least spam possible.

What about the government and the CAN-SPAM Act? Won't that take care of the Spam problem? Do I really need your software?

The CAN-SPAM Act, which was just recently made law in the United States protects citizens from the tide of spam by requiring commercial emails to have a working "Unsubscribe" button or link in it. Failure to comply would result in criminal charges. A conviction would mean fines and/or prison time. This is a wonderful development in the fight against spam, but it has its problems.

While the details of the enforcement of such a law are being rolled out, you will continue to get spam today. And once the law has truly taken effect, you will still have to MANUALLY opt out – meaning you will have to spend more time clicking on links in spam and filling out forms just to unsubscribe. For most of us, this means that we'll have to spend more time than ever on spam, just to take advantage of the new law.

LashBack AUTOMATICALLY unsubscribes you from messages identified as spam. With one-button, you block the sender, filter future messages from that sender and automatically find their unsubscribe form to fill it out.

Doesn't 'Opting-Out' just let the spammers know my email address is valid and ultimately get me more Spam?

Some spammers make fake unsubscribe buttons/links and use clicks to determine which email addresses are valid – so they can continue to spam them.

LashBack addresses this possibility with a 'Trust System' which identifies email advertisers as Trusted (someone known to honor Unsubscribe requests), Untrusted (someone who is known to abuse the requests to send more spam), or Unknown.

Advertisers begin as labeled 'Unknown,' during which time your Opt-out requests are recorded by the LashBack servers but are not sent. Instead, LashBack sends out a 'probe' (an opt-out request by the server) to test to determine if the process is safe. If it's safe, the advertiser becomes Trusted and your request is processed. If it is unsafe (they send back spam), they become Untrusted and your request is not sent (you simply block and filter them, while LashBack gathers evidence of their illegal activity). If LashBack cannot determine either way (say, the link is broken), your opt-out request is held while additional testing is conducted.

This Safe Unsubscribe feature is patent-pending.

How LashBack Works

How does LashBack stop spam?

LashBack's approach to fighting spam is a multi-tiered attack. When you highlight a message and click on the red LashBack lightning bolt button on your email client's toolbar, several things all happen at once:

- The message is removed from your inbox and is placed in a custom "Spam" folder.
- The sender of that message is added to your "Blocked" List. Future messages from that sender are prevented from reaching your inbox.
- LashBack gets a copy of the spam message from you, records it, scans it and then (based on the website they're advertising), filters all messages that advertise the same product or service.
- If the advertiser's Unsubscribe mechanism is considered to be Trusted, you are automatically unsubscribed from that spammer's email list.
- The unique and simple combination of these actions eliminates the spam you have today and prevents you from getting spam tomorrow (and on).

If one button does all the work, what do the other three buttons do?

The other three buttons are:

- Add To SafeList - Highlight a message and click this button to add a relative, friend, coworker or other trusted source to a list of addresses which guarantees messages from those email addresses will always be delivered successfully to you.
- Configure - Change your personal options, review your blocked list, initiate a scan for spam in your inbox and much more.
- Reports - Launches our Spam Control program which can let you run reports to determine what messages are being filtered, who's sending them, which ones are honoring your opt-out requests and more.

Does LashBack do anything to discourage spammers from sending me spam in the first place?

In addition to blocking, filtering and unsubscribing you from spam, LashBack also uses the information it gathers on the illegal activities of spammers to work with anti-spam organizations worldwide to find and punish spammers for their criminal activities. In this way, LashBack Community members (subscribers) are all contributing to the end of spam as we know it. This is precisely how you are able to 'lash back' against spam.

Setup, Cost and Upgrades

How hard is it to set LashBack up? How hard is it to use?

LashBack is designed with the Beginner in mind. We figure spam is annoying enough without it becoming MORE complicated to get rid of it. We want using LashBack to be as easy as using the delete key, only a LOT more powerful in the fight against spam.

Installation and setup takes less than five minutes. A quick interactive tutorial is included to go over all of the most commonly-used functions and an online manual covers everything else you might need to know.

How much does LashBack cost to use?

The LashBack toolbar costs absolutely nothing to use. Updates to the service, upgrades to the product and technical support are all included for free.

Does LashBack work with Macintosh or Unix computers?

No, we do not currently support those operating systems. We do, however, have plans to offer these options in the future.

I don't use Outlook or Outlook Express for my email, but I want to try LashBack. Do you have plans to release other editions of the software to cover other email clients like Eudora, MSN, AOL or Hotmail?

Other versions are continually in the works! If you would like to be notified when new versions become available, you can join our mailing list by contacting us at updates@lashback.com with "new versions" as the subject line.

Technical Questions

I have more than one email address. Will LashBack work with all of those email addresses at once, or…?

LashBack protects all email addresses used by one computer (that are configured for use with email clients we support). A separate copy of LashBack is required for additional computers, but not for additional email addresses.

How much of my computer's resources will LashBack be using? Will it affect the other things I already do on my computer?

While the amount of processing power devoted to LashBack is customizable, most users will default to the same amount of processing power and internet bandwidth usage as would be required to view a simple web page. In other words, you are highly unlikely to notice any diminishment in processing power or internet speed.

Will Lashback ever block or filter 'good' email?

While it is unlikely, it is possible that while you begin to use the Filtering offered by LashBack, some email from trusted sources may diverted incorrectly into the Spam folder. If this happens, simply highlight the message in your spam folder and click on “Add to SafeList” so that any message from that email address will always be allowed to go into your inbox.

It is highly recommended that you add all friends, family and other trusted email addresses to your SafeList as soon as you install LashBack to ensure the best possible filtering results.

How can I add someone to my SafeList if I don't already have an email of theirs to highlight?

On the LashBack toolbar, click on “Configure” and choose the “Spam Control" button (alternately, you can double-click the Lashback icon in your system tray). Click on the green SafeList button to access the list of trusted addresses. Then, click on “Add” and type in the email address to be added. Click OK and you’re done!

© 2003-2007 LashBack, LLC.
555 Washington Ave. Suite 400, St. Louis, MO 63101
(800) 434-1994

The Wayback Machine - https://web.archive.org/web/20090130004220/http://www.lashback.com:80/reputation/



Reputation
Data Story
Reputation Toolbox
Unsubscribe Best Practices
Blacklist Resources

Feature Comparison Chart

Reputation

Are You Trusted or Untrusted?

A critical part of the LashBack mission is to define the working relationship between compliancy, reputation, deliverability and increased revenue in a best practices context.

The industry standard used to determine deliverability of your email is your reputation. Your reputation takes the form of a score, not unlike a personal credit score and is used by receivers such as Yahoo!, AOL, MSN and all major ISP's to determine whether your email gets delivered. The score is based on a 0 to 100 scale. 100 is perfect and 0 is poor. If you have one case of unsubscribe abuse your score will drop to 0. Even if it not your fault. This shows the need to know who you are working with and who is affecting your business positively with compliance and negatively with non-compliance.

The popular authentication services require a 90 on the 100 point scale. It is difficult, if not impossible to maintain this high reputation score without a comprehensive compliance process.

The unsubscribe portion of your reputation score is determined directly by LashBack and this data, based on the performance of your unsubscribe compliance is shared with receivers through LashBack reputation service partners such as Return Path, Cloudmark, MX Logic, Truste, Unsubscentral and Habeas.

Your reputation has a direct effect on your revenue. If your deliverability suffers from a poor reputation, then your bottom line decreases proportionately. The good news is the reverse is also true. By monitoring your compliancy and adherence to internal standards you can maintain and increase a good reputation. More email delivered means more revenue.

Compliance means reputation and reputation is deliverability.

Unsubscribe, CAN-SPAM and Your Reputation

The CAN-SPAM Act is "opt out" legislation. It does not stop any company from sending anyone compliant commercial email but, if they opt out of your list, it is illegal to send them more email after 10 days. This makes unsubscribe the most critical aspect of CAN-SPAM. The legislative intent of CAN-SPAM as enforced by the FTC is to allow an "email marketplace" where a consumer can opt-out or unsubscribe safely.

LashBack shares this unsubscribe perspective as "The Unsubscribe Authority" of email. As we have grown to become the clear "Email Compliance Authority", LashBack has documented hundreds of unsubscribe mechanisms and processes. UnsubMonitor watches hundreds of thousands of unsub mechanisms and documents their performance through the use of comprehensive, patent-pending technology.

Where to start:

Do you know what your reputation score is?
Do you know the 10 guidelines to check for to ensure CAN-SPAM Compliance?
Do you know what violations you have had?

© 2003-2007 LashBack, LLC.
555 Washington Ave. Suite 400, St. Louis, MO 63101
(800) 434-1994

The Wayback Machine - https://web.archive.org/web/20090131072826/http://www.lashback.com:80/reputation/UnsubscribeBestPractices.aspx

Unsubscribe Best Practices

Confirming Unsubscribe Requests

LashBack does not support nor recommend a double-opt out process. Consumers wishing to unsubscribe from receiving email from you should not have to receive more email from you in order to stop receiving email from you. However, email notices of a successful opt-out request are recommended.

Unsubscribe Links vs. Unsubscribe Mechanisms

It is important that the distinction between unsubscribe links and unsubscribe mechanisms be made. An unsubscribe mechanism is the final email address or web page that an unsubscribe request is submitted to, ignoring any parameters. An unsubscribe link is the link the user selected to reach that mechanism. For email-based unsubscribes, the unsubscribe mechanism and unsubscribe link are considered the same. However, in web cases, the link clicked in an email (the unsubscribe link) and the ultimate page the unsubscribe is posted to (the unsubscribe mechanism) is generally different. The following example clarifies the distinction between and unsubscribe link and an unsubscribe mechanism:

Step 1 - Consumer clicks the following link in an email to unsubscribe:
http://www.domain.com/unsubscribe.htm

Step 2 - Consumer is automatically redirected to another page to fill in an email address and submit a form to unsubscribe:
http://www.domain.com/unsubscribeform.htm

Step 3 - Consumer submits the unsubscribe form which is posted to:
http://www.domain.com/processunsubscribe.cgi

Step 4 - Consumer is taken to a confirmation page indicating a successful unsubscribe:
http://www.domain.com/unsubsuccess.htm

In the above scenario, http://www.domain.com/unsubscribe.htm is considered the unsubscribe link and http://www.domain.com/processunsubscribe.cgi is considered the unsubscribe mechanism.

Ensuring LashBack Can Find your Unsubscribe Link

There are currently no standard labeling practices in the world of email unsubscribe. In order to find your unsubscribe link, LashBack uses multiple approaches, some of which involve human identification. The easier it is for LashBack to locate your unsubscribe link, the more likely you will have a good reputation with LashBack. Some general recommendations to ensure LashBack is able to find your unsubscribe link are as follows:

- Use a List-Unsubscribe header as described in RFC 2369
- In the case of email-based unsubscribe links included in the body of the email message, include the word ‘unsubscribe’ in the email address itself (e.g., unsubscribe-newsletter1@domain.com)
- In the case of web-based unsubscribe links included in the body of the email message, include the word ‘unsubscribe’ in the unsubscribe link (e.g., http://www.domain.com/unsubscribe-newsletter1.cgi or http://www.domain.com/unsubscribe/newsletter1.cgi)

Ensuring LashBack Can Use your Unsubscribe Link

Equally important to finding your unsubscribe link, LashBack must be able to easily and reliability navigate and use your unsubscribe link. Some general recommendations are listed below:

- Use an email-based unsubscribe link and make sure the actual recipient's email address (and only this email address) is specified in the TO: header. If both of these conditions are met, LashBack will always be able to reliably use your unsubscribe link.
- Web-based unsubscribe links should be hosted on a single web page (i.e., users should not have to navigate multiple pages to unsubscribe).
- Web-based unsubscribe links should pass in all required unsubscribe parameters or only require the consumer's email address to unsubscribe.
- Web-based unsubscribe links should require users to click a button to confirm the unsubscribe request. Automatically unsubscribing user's by simply clicking the unsubscribe link is not recommended.
- Web-based unsubscribe links should provide the consumer confirmation of a successful unsubscribe which includes the words 'unsubscribe' and 'successful'.
- Web-based unsubscribe links should not use or require active scripting to function (JavaScript or VBScript).

Changing Unsubscribe Mechanisms

Every time a sender changes unsubscribe mechanisms, LashBack checks to see if the sender has used the mechanism in the past. If the sender has not used the mechanism in the past, all UnsubSafe processing is suspended while LashBack tests the safety of the new mechanism. This is to ensure consumers are protected from potential misuse of their unsubscribe request. Senders wanting to ensure UnsubSafe is enabled should avoid switching unsubscribe mechanisms often. Senders can change their unsubscribe link as often as they like without suspending UnsubSafe so long as the ultimate unsubscribe mechanism remains constant.

Testing Your Unsubscribe Link with LashBack

To assist senders in checking to ensure LashBack is able to find and use their unsubscribe link, LashBack provides a simple method to do so. Simply send a message with your advertisement or newsletter to unsubcheck@unsubsafe.com. Within 5 minutes of receiving the message, an email message will be returned to the sender of the email (the FROM: address) with results indicating whether LashBack was able to a) find your unsubscribe link and b) use your unsubscribe link. If you are having problems getting your unsubscribe link to work with LashBack, LashBack may be able to assist you with making changes.

Expectations for Segmenting Unsubscribes

While the CAN SPAM Act dictates that senders must provide consumers an option to opt out, it is sometimes unclear about what unsubscribe options should be provided to consumers and how unsubscribe requests should apply within. LashBack's unsubscribe segmentation expectations are designed to match consumer expectations. However, LashBack does not warranty that the segmentation expectations here will protect senders from legal liability under the CAN SPAM Act. Senders and advertisers should always consult legal counsel in making these policy decisions. When in doubt, Senders should err on the side of caution and treat requests globally.

Opt In Communications
In general, unsubscribe segmentation should match opt-in segmentation. For example, if a consumer explicitly signs up for a newsletter with an organization, then a consumer would expect that an unsubscribe request would eliminate this future correspondence. In cases where a consumer has opted in for general communication from your organization but this was not specific to a specific type of communication, then opt out requests should be treated globally in the organization.

Acquisition Emails
All emails sent advertising products or services to customers that do not have a preexisting relationship with the actual seller/provider of the product of service. In cases of acquisition email, all unsubscribes should be applied globally within the organization. If there are two parties involved in the transmission of the email – a sender and an advertiser – both parties should provide a global unsubscribe link accessible from the email sent. Segmenting unsubscribes by offer, brand, domain or other method is not accepted to qualify for UnsubSafe.

Mirror Unsubscribe Mechanisms with Unsubscribe Segmentation
LashBack uses several techniques to determine when a sender or advertiser is not honoring unsubscribe requests. One of the primary techniques LashBack uses to identify repeat attempts for a consumer to unsubscribe using the same unsubscribe mechanism after 10 business days

(failure to honor). Senders and advertisers should be aware of this, since using the same unsubscribe mechanism for multiple lists may cause false positives in their unsubscribe reputation. LashBack CSRs review all unsubscribe issues to confirm the problem, but senders should be aware of the problems this may cause. LashBack recommends all senders and advertisers to use unique unsubscribe mechanisms to match unsubscribe segmentation expectations set forth above. However, it should be reiterated that senders or advertisers that constantly change unsubscribe mechanisms will either have a poor reputation or no reputation and will not qualify for UnsubSafe.sts globally.




© 2003-2007 LashBack, LLC.
555 Washington Ave. Suite 400, St. Louis, MO 63101
(800) 434-1994



Reputation
Data Story
Reputation Toolbox
Unsubscribe Best Practices
Blacklist Resources

Feature Comparison Chart

Reputation Toolbox

Building Reputation

LashBack leverages consumer unsubscribe requests to build sender reputation. If LashBack does not have sufficient historical data about a sender or the sender has a poor historical unsubscribe performance, then these senders are not provided an UnsubSafe option for consumers to use. Those senders wishing to build a good reputation or that have a poor historical reputation with LashBack can easily build reputation by adding a series of 'seed' email addresses to their send list. LashBack processes unsubscribe requests on these seeds as mail is sent to them in a staggered pattern and senders are only given credit for an unsubscribe when email is sent to the remaining seeds.

Manual Seed Insertion

Senders wishing to manually generate a list of seeds and insert them into their send list can get this list here. These email addresses should be inserted directly into your list and not be removed until they are unsubscribed. It is recommended that senders consider doing this on a monthly or quarterly basis using the UnsubSafe Seed Generator.

Seeding API

Email Service Providers and other entities interested in automatically adding seeds to their send list can programmatically do so using LashBack's Seeding API. For the parameter "strClientKey", please use a value that will help us to identify your organization. The function call returns a comma-delimited list of email addresses that should be added to your send list. The Seeding API may be found at the Reputation Seed List Generator

Checking Reputation

Senders wishing to check whether UnsubSafe is enabled can do so by going to our UnsubSafe checker and entering their IP address. This can be accessed at the UnsubSafe Lookup

Research your Partner's Unsubscribe Links

Senders wishing to check the unsubscribe links of their partners to ensure they do not have suppression list abuse can do so at the Untrusted Unsubscribe Lookup

LashBack's UnsubScore Abuse Reset Policy

The owner of an IP may request removing abuse from a sending IP's UnsubScore if:

1. The mail message sent by the IP that initiated the probe was sent more than 90 days ago
2. The sender attests that they have either:
A. Discontinued working with the advertiser associated with the abuse OR
B. The advertiser associated with the abuse has proven to the sender that they are protecting suppression lists through hashing techniques or are no longer publishing raw suppression lists

Reset requests must be made by sending an email to cs@lashback.com . The request must include the IP(s) to reset, the advertiser(s) responsible, and indication of what action the sender

has taken with the advertiser (a or b above).

Reset requests are only allowed once per advertiser per sender. If the problem happens again for the same advertiser, the sender will have to wait for the abuse to fall off naturally. The natural fall off period is 90 days after mail is sent to LashBack's unsubscribe seed address.

LashBack clients and non-clients are both allowed these requests. However, client requests will be processed in 1 business day while non client requests will be processed within 5 business days. Non-clients are only allowed one request every three months

© 2003-2007 LashBack, LLC.
555 Washington Ave. Suite 400, St. Louis, MO 63101
(800) 434-1994

The Wayback Machine - https://web.archive.org/web/20090202091204/http://www.lashback.com:80/reputation/BlacklistResources.aspx



Reputation
Data Story
Reputation Toolbox
Unsubscribe Best Practices
Blacklist Resources

Feature Comparison Chart

Inc. 2007 Best of Technology
CAN-SPAM Compliance Monitor
for making sure your outbound email works

Unsubscribe Blacklist (UBL) Resources

What is the UBL?

The Unsubscribe Blacklist (UBL) is a real-time blacklist of IP addresses which are sending email to names harvested from suppression files.

Statistics

New IPs in the last 48 hours	0
IPs Removed in the last 48 hours	19,370
Delist Requests in the last 48 hours	55
Total IPs Listed	894,766

Quick Links

How to perform DNS lookups
UBL via XML
UBL via TXT
UBL in RBLDNSD Format
RSYNC Access
Research IPs listed on UBL
Blacklist Delist Procedure
Research URL Reputations
How to Build a Good Reputation

About the UBL

Utilizing the world's largest unsubscribe intelligence database, LashBack's Unsubscribe Blacklist (UBL) empowers your organization to identify and block the very worst unsubscribe abusers; those that send email to addresses which have been harvested from suppression lists.

LashBack has been monitoring sender unsubscribe compliance since 2003. During this period, LashBack has compiled sender unsubscribe compliance failure in four primary categories:

1. Which senders fail to provide a working unsubscribe mechanism
2. Which senders do not honor unsubscribe requests within 10 business days
3. Which senders allow consumers unsubscribe request to be abused (i.e., shared with other parties to send more spam)
4. Which senders are taking suppression lists from other organizations and sending email to these lists

LashBack's UBL only lists the IP addresses of senders who are using email addresses harvested from suppression lists (point 4). If you would like additional "premium" reputation data contact a LashBack representative directly.

This free service is intended to provide all receivers and reputation providers a baseline of data to help block the sender's with the worst reputations. All IP addresses listed on in our service are being continually monitored and the list is updated hourly.

Web Lookup

To perform ad-hoc lookups or to delist an IP for the first time, please visit the UBL Lookup and delist page.

XML Download

If you wish to download an XML copy of the blacklist, this file is available at the XML UBL download link. This XML file is updated hourly with the latest blacklist data.

Text Download

If you wish to download a text copy of the blacklist, this file is available at the text UBL download link. This text file is updated hourly with the latest blacklist data.

RBLDSND Format Download

If you wish to download a copy of the blacklist in RBLDNSD format, this file is available here. This file is updated hourly with the latest blacklist data.

RSYNC Access

All downloadable files are available via RSYNC at:
rsync://rsync.unsubscore.com/LBBL/blacklist.xml (XML)
rsync://rsync.unsubscore.com/LBBL/blacklist.txt (TEXT)
rsync://rsync.unsubscore.com/LBBL/ubl_rbldns.txt (RBLDNSD)

DNS Lookups

This service is a list of hostnames in the ubl.unsubscore.com zone. These hostnames may appear to be real IP Addresses. However, they are hosts in the ubl.unsubscore.com DNS zone.

In order to check whether an IP is listed in the UBL, you can perform a DNS query using the IP address of the sender. However, you must reverse the IP address in order to perform the query. For example, if you wish to check whether 192.168.1.100 is listed in the UBL, you would perform a DNS lookup on 100.1.168.192.ubl.unsubscore.com. If one of the DNS return codes listed below is returned, then the IP is listed in the UBL.

UBL Return Codes

Currently the LashBack UBL supports the following return codes. Please note that LashBack will likely continue to add additional return codes over time.

127.0.0.2 - This return code indicates that the IP address has sent to email LashBack unsubscribe probes. These senders are taking email addresses from unsubscribe requests and spamming them.

Zone Transfers

Currently the UBL allows anonymous zone transfers of ubl.unsubscore.com.

Mail Server Configuration

The LashBack UBL can be used for any mail server supporting connection level blacklists. The blacklist server should be set to ubl.unsubscore.com.

Delisting Requests

LashBack will actively address any requests to be delisted. Before sending us a delist request, please visit the UBL Lookup and delist page, where you may delist the IP at the click of a button.

Data Use Restrictions

The UBL database is provided free for both commercial and non-commercial use.

DISCLAIMER OF WARRANTIES AND LIABILITY

All data is provided for your personal information only, and not intended for legal purposes. LashBack LLC is not liable for any errors in the data, or for any actions taken in reliance thereon.

LASHBACK LLC MAKES NO WARRANTY, EXPRESSED OR IMPLIED, AS TO THE RESULTS TO BE OBTAINED BY ANY USER OR OTHERS FROM THE USE OF THE INFORMATION PROVIDED HEREUNDER. LASHBACK MAKES NO EXPRESS OR IMPLIED WARRANTIES OF FITNESS OF THE INFORMATION FOR A PARTICULAR PURPOSE OR USE.

The information contained in LashBack databases has been developed by LashBack and are considered by LashBack to be reliable. However, the accuracy and completeness thereof are not guaranteed and LashBack and its data suppliers shall have no liability for errors or omissions regardless of the cause or source of such error or omission.

LASHBACK LLC DOES NOT HAVE ANY LIABILITY TO A USER OR TO OTHERS FOR ANY LOST PROFITS OR INDIRECT, SPECIAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES, EVEN IF ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES.

LashBack may change or discontinue the databases, or their availability to you, at any time without notice.

© 2003-2007 LashBack, LLC.
555 Washington Ave. Suite 400, St. Louis, MO 63101
(800) 434-1994

The Wayback Machine - https://web.archive.org/web/20090131072744/http://www.lashback.com:80/reputation/DataStory.aspx

Data Story: Return to Sender

Where Does LashBack Data Come From? How are you "always watching"?

The Power of the LashBack Compliance FeedBack Loop is derived from real-world consumer data. LashBack receives data from many valuable sources. The most valuable data is from the free LashBack consumer toolbar for Outlook and Outlook Express (link to New consumer toolbar download page.) The toolbar provides an automatic check of the reputation of the owner of the unsubscribe mechanism, which enables consumers to unsubscribe safely from unwanted email.

LashBack also works with a number of ISPs, anti-spam organizations and ESP's who feed LashBack monitors a data stream of email for analysis. LashBack is analyzing over 150,000 pieces of actual consumer emails on a daily basis. The data stream is real-world and uniquely consumer driven. The LashBack relationship to consumer inboxes is the most vital relationship our client's leverage.

The very best reputation management services companies and receivers utilize LashBack's unique data as part of the reputation score with which they each rate senders.

This process is also called a "feedback loop" which all email marketing experts agree email senders need to be a part of to understand the actual performance of their email marketing programs.

© 2003-2007 LashBack, LLC.
555 Washington Ave. Suite 400, St. Louis, MO 63101
(800) 434-1994

The Wayback Machine - https://web.archive.org/web/20090131154140/http://www.lashback.com:80/products/UnsubSafe.aspx



Overview
UnsubMonitor
CAN-SPAM Monitor
BrandAlert
UnsubSafe
Get a Demo

Feature Comparison Chart

ISP and Receiver UnsubSafe

The First and Only

Simply filtering junk email only hides the problem. To truly receive relief from the ever increasing flood of junk email sent to your customers through your network, LashBack brings you its revolutionary new UnsubSafe service. Available to Internet Service Providers and anti-spam firms free of charge, UnsubSafe immediately reduces the amount of junk email sent to you and your customers each day.

In order to determine which email marketers can be trusted with your unsubscribe request, the UnsubSafe service automatically searches though its massive database of email marketer's reputations and extracts an UnsubScore. Based on the score that is returned by UnsubScore, LashBack knows when it's safe to unsubscribe and when requests should be safely kept away from un-trusted email marketers.

More than One Way to UnsubSafe

Option 1

If you currently allow your customers to report spam, you can simply forward a copy of these messages to LashBack via secure SMTP. Alternatively, if your network already filters out spam messages sent to your customers, you can simply forward a copy of filtered message to LashBack. In either case, LashBack will parse through those messages to extract the email marketer's identity and unsubscribe reputation, or UnsubScore. If the email marketer has a good reputation, LashBack will automatically and safely unsubscribe your customer from future mailings. If the email marketer has a bad unsubscribe reputation, the unsubscribe attempt is suppressed.

UnsubSafe SDK Documentation
Is your business ready for UnsubSafe? Contact Us.

Option 2

If your organization doesn't already have a network-level spam filtering service deployed, or you would like to extend spam reporting all the way to your customer, LashBack can integrate a customizable reporting toolbar that is directly installed into the customers email client (Outlook and Outlook Express).

Deploying the UnsubSafe toolbar solution allows your organization the opportunity to increase the perceived value of your service by enabling your customers to see and experience the value of UnsubSafe first hand. Additionally, customization of the toolbar with your organization's logo further deepens the bond between you and your customers.

"89.7% of respondents agreed that they would prefer that their ISP or email service provider include an unsubscribe option that would safely remove them from email lists"
Bigfoot Interactive - Spam Research Survey

Expand your Spam Intelligence
Optionally, when you deploy the UnsubSafe toolbar on your network, you can have a copy of all messages reported on your network sent back to you for review. This data can be used by your

to gauge the impact and success of your current filtering solutions as well as additional intelligence to maximize your networks catch rate and filtering performance.

Reporting
Real-time Unsubscribe Performance reports are made available so you can see the value and impact LashBack is having on your organization's junk email problem. At a glance, you'll be able to review network level statistics and unsubscribe requests as well as additional data you can use to drill into any specific spam report and view each email marketers' UnsubScore and the messages they sent your customers.

Contact LashBack Sales at 800.434.1994

To learn more about Option 2, contact us.

© 2003-2007 LashBack, LLC.
555 Washington Ave. Suite 400, St. Louis, MO 63101
(800) 434-1994

LashBack: UnsubSafe SDK
Version 1.0
LashBack's UnsubSafe service allows ISPs and anti-spam firms to send unsubscribe requests to LashBack for safe processing. The actual implementation of this service will depend on the preferences of the organization and its customers. Some common implementations, with their pros and cons, are outlined below:

1) **One-Click UnsubSafe – 'Always On'**
   An unsubscribe button is always presented in the UI. When viewing a specific email message, a consumer can click this button, initiating the UnsubSafe process.

   Pros:
   -An 'always on' option allows a wider range of reputation data to be compiled. This benefits future deliverability decisions.

   -An 'always on' option allows for improved internal filtering decisions, since you can differentiate 'Report as Spam' decisions from unsubscribe decisions.

   Cons:
   -An 'always on' option may create confusion with consumers, since an unsubscribe request will only be processed when it is safe to do so.

   With this option, only the UnsubSafe API is employed.

2) **One-Click UnsubSafe – 'Toggled'**
   An unsubscribe button is only presented in the UI when the sender's UnsubScore is above a pre-determined value. When viewing a specific email message and the button is enabled, a consumer can click this button, initiating the UnsubSafe process.

   Pros:
   -A 'toggled' option will limit consumer confusion, since unsubscribes will generally always be processed as received, since the sender's reputation is already established.

   Cons:
   -A 'toggled' option limits the amount of reputation data that can be collected on an ongoing basis.

   -A 'toggled' option will inhibit your ability to differentiate 'Report as Spam' decisions from unsubscribe decisions.

   With this option, both the UnsubSafe and UnsubScore APIs are employed.

3) **Seamless UnsubSafe – 'Always On'**
   No unsubscribe button is presented to the user. Instead, UnsubSafe is integrated with existing 'Report as Spam' functionality in the UI. As consumers report spam, a copy of the message is sent for UnsubSafe processing.

   Pros:
   -Seamless integration removes the need for consumers to make a distinction between 'Report as Spam' and unsubscribe

-An 'always on' option allows a wider range of reputation data to be compiled. This benefits future deliverability decisions.

Cons:
-An 'always on' approach will create additional volume sent to UnsubSafe, when some reports may not be able to be processed.

With this option, only the UnsubSafe API is employed.

4) **Seamless UnsubSafe – 'Toggled'**
No unsubscribe button is presented to the user. Instead, UnsubSafe is integrated with existing 'Report as Spam' functionality in the UI. As consumers report spam, a copy of the message is sent for UnsubSafe processing when the sender's UnsubScore is above a pre-determined value.

Pros:
-Seamless integration removes the need for consumers to make a distinction between 'Report as Spam' and unsubscribe

-A 'toggled' option will only send a copy to UnsubSafe when an unsubscribe request can be safely processed, reducing overall message volume.

Cons:
-A 'toggled' option limits the amount reputation data that can be collected on an ongoing basis.

With this option, both the UnsubSafe and UnsubScore APIs are employed.

UnsubSafe APIs
The UnsubSafe APIs provide a mechanism to report messages to LashBack for UnsubSafe processing. There are currently two APIs for reporting messages for processing. The SMTP method is preferred, but both APIs are offered.

SMTP
This is the preferred method for reporting messages to UnsubSafe for processing. UnsubSafe clients will be provided an SMTP address to forward messages to. UnsubSafe processing requests are simply forwards of the full message and headers in RFC 822 format. In addition, the following field tags should be appended to the top of the message.

[LBUS_VERSION:1.0]
This value indicates the UnsubSafe API version you are using. The current API version is 1.0. This field value is required.

[LBUS_CLIENT_KEY:XXX]
When you sign up for UnsubSafe, you will be provided a unique client key. This key must be specified in this field or the UnsubSafe request will be rejected. This field value is required.

[LBUS_MTA_IP:XXX.XXX.XXX.XX]

This is the IP address of the MTA that sent the mail. If this address is not known, the field value should be left blank.

[LBUS_EMAIL_ADDRESS:XXX@XX.XXX]
This is email address of the actual recipient. This value is especially useful when dealing with newsletters sent to groups. If this value is not known or not available, the value should be left blank.

[LBUS_SPF_SENDERID_DOMAIN:XXXX.XX]
If you have performed SPF/SenderID checks on the message and have confirmed the authenticated domain, this domain value should be listed here. Otherwise, the value should be left blank.

[LBUS_DK_DOMAIN:XXX.XX]
If you have performed a DomainKeys check on the message and have confirmed the authenticated domain, this domain value should be listed here. Otherwise, the value should be left blank.

An example UnsubSafe request is listed below:

```
[LBUS_VERSION:1.0]
[LBUS_CLIENT_KEY:samplekey3332$]
[LBUS_MTA_IP:72.11.144.121]
[LBUS_EMAIL_ADDRESS:testemail@lashback.com]
[LBUS_SPF_SENDERID_DOMAIN:]
[LBUS_DK_DOMAIN:]
Return-Path: <Davenport@alch.golfshore.com>
Received: from 121.golfshore.com ([72.11.144.121]) by ns1.plexis.net
        (Post.Office MTA v3.5.3 release 223 ID# 0-70569U1000L2S100V35)
        with ESMTP id net for <testemail@lashback.com>;
        Sat, 12 Mar 2005 02:40:51 -0500
From: Home Makeover<Davenport@alch.golfshore.com>
To: testemail@lashback.com
Subject: Win a Dream Home Makeover
Date: 12 Mar 2005 02:31:41 -0500
Message-Id: <2265281@lha_enY-ydkkydkkxehh>
Click to win a $50,000 Kitchen & Bath Make-Over!
--or take the cash
http://alch.golfshore.com/ATGV1111_4/123/soh_luF/fkrrfkrreloo/u.htm

You'll also get:

-Free Samples
-Grocery Coupons
-Store Coupons

Click here:
http://alch.golfshore.com/ATGV1111_4/123/soh_luF/fkrrfkrreloo/u.htm
```

Web Service

As an alternative to SMTP, messages can be submitted for UnsubSafe processing via a web service. A definition of this web service can be found at: http://www.lashback.com/us/v1.0/unsubsafe.asmx?op=SendToUnsubSafe

The SendToUnsubSafe operation will send a message to UnsubSafe for processing. The parameters of this operation are described below:

strLBMUS_MTA_IP
This is the IP address of the MTA that sent the mail. If this address is not known, the field value should be left blank.

strLBMUS_EMAIL_ADDRESS:
This is email address of the actual recipient. This value is especially useful when dealing with newsletters sent to groups. If this value is not known or not available, the value should be left blank.

strLBMUS_SPF_SENDERID_DOMAIN
If you have performed SPF/SenderID checks on the message and have confirmed the authenticated domain, this domain value should be listed here. Otherwise, the value should be left blank.

strLBMUS_DK _DOMAIN
If you have performed a DomainKeys check on the message and have confirmed the authenticated domain, this domain value should be listed here. Otherwise, the value should be left blank.

strLBMUS_CLIENT_KEY
When you sign up for UnsubSafe, you will be provided a unique client key. This key must be specified in this field or the UnsubSafe request will be rejected. This field value is required.

strLBMUS_REPORT
Full email message and headers in RFC 822 format.

Return Codes
The web service returns an integer value. The returns codes are as follows:
0 = Failed Submission
1 = Successful Submission

The FetchReputationSeedList function returns a comma delimited string of randomly generated email seeds. The seeds are designed to be inserted into mailing lists of senders that wish to build a reputation with LashBack. When created, each seed is assigned a random date. After each date is expired, LashBack will attempt to unsubscribe those seeds and test their results. A definition of this function may be found at: http://www.lashback.com/us/v1.0/unsubsafe.asmx?op=FetchReputationSeedList.

The parameters of this operation are described below:

strClientKey
This is a required string that is currently used for information gathering purposes only. In the future it will be used as a license key to allow or deny access to this service in order to limit its usage to registered users.

Return Codes
The web service returns a comma-delimited list of email addresses when successful. If the process fails, it will return an empty string.

UnsubScore API
In implementations where an Unsubscribe option is toggled based on the unsubscribe reputation of the sender, the UnsubScore API allows you to look up the reputation of the sender to make this determination.

Web Service
A web service is provided to UnsubSafe clients to lookup the unsubscribe reputation of a sender. A definition of this web service can be found at:
http://www.lashback.com/us/v1.0/unsubsafe.asmx?op=CheckUnsubScoreByIP

The CheckUnsubScoreByIP operation will indicate whether a given sender should be trusted with an unsubscribe request, based on the input parameters. The parameters of this operation are listed below:

strLBMUS_MTA_IP:
This is the IP address of the MTA that you wish to check

dblLBMUS_SCORE_THRESHOLD
This is the minimum value an UnsubScore must be for you to trust the sender. This field is a double and accepts values of between 0.00 and 100.00. An UnsubScore of 0 means that a particular sender cannot be trusted with an unsubscribe request, while an UnsubScore of 100 means that the sender's track record it to always accept and honor unsubscribe requests.

strLBMUS_CLIENT_KEY
When you sign up for UnsubSafe, you will be provided a unique client key. This key must be specified in this field or the UnsubSafe request will be rejected. This field value is required.

Return Codes
The web service returns an integer value. The returns codes are as follows:
0 = Failed submission
1 = Sender is safe based on UnsubScore threshold
2 = Sender is not safe based on UnsubScore threshold
3 = Insufficient data on sender to make determination

Sample Implementation

Overview
An ISP currently provides its customers with web-based email access. The ISP already employs spam filtering on its customer's incoming email and most items known to be spam are automatically moved to this folder as they come in. In addition, the ISP offers consumers the ability to click a 'Report Spam' button on a message they are viewing if they believe the message is spam. The ISP uses the spam reports made by customers to help make better decisions about what spam is in the future.

The ISP has decided to implement UnsubSafe into its web-based mail interface. The ISP feels that there is perceived value by its customer to have a separate button for 'Unsubscribe' versus 'Report as Spam' so the ISP has opted to add an 'Unsubscribe' button to their UI. In addition, the ISP feels that being able to differentiate 'Report as Spam' decisions from 'Unsubscribe' decisions should make its future filtering efforts more reliable.

However, the ISP feels that the best implementation of the 'Unsubscribe' button in its UI is to toggle the button. The ISP only wants the button to display this button when the customer is viewing a message from a sender that has a good unsubscribe reputation.

Implementation Details
In this implementation scenario, the ISP must integrate both the UnsubSafe and UnsubScore APIs.

Toggling the Unsubscribe Button
First, the ISP must add an Unsubscribe button to their web UI. To do this, the ISP's development team altered the code of the web page that loads when a customer is viewing an email message. As a specific email message is viewed by a customer, the code of the web page makes a web service call to the UnsubScore API. Specifically, the CheckUnsubScoreByIP operation is called by the web page, passing in the IP address of the email message sender, as well as the required UnsubScore a sender must have in order for an unsubscribe request to be considered safe. The call to this operation will return a value to indicate whether an Unsubscribe request can safely be processed for this sender. If the value returned indicates a user can safely unsubscribe (a return code of 1), then the code behind the page automatically enables the Unsubscribe button. When the page loads, the customer will then see the available Unsubscribe button.

Handling Unsubscribe Requests
In this implementation, the ISP has decided to send UnsubSafe requests using the specified SMTP API. As customers press the Unsubscribe button, a corresponding web page takes a copy of the email message and formats it in the format specified in this document. Once the request is sent for UnsubSafe processing, a web page is displayed to the customer indicating their unsubscribe request has been sent.