Improving E-mail Deliverability into Windows Live Hotmail

Microsoft

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Table of Contents

Introduction

Understanding Deliverability Issues

The document serves to provide an overview of the services, resources and best practices that marketers and online advertisers may utilize to improve their deliverability into Windows Live Hotmail and other receiving networks. As the tactics employed by spammers and deceptive mailers change, technologies, policies and processes will evolve to support the primary goal of improving end-user trust and confidence in e-mail and the Windows Live Platform. The content contained in this document should be considered current as of the time of publication, but is not a guarantee of delivery to the inbox. Senders are recommended to periodically visit www.microsoft.com/postmaster for updates.

The Internet and e-mail have become a vital platform for communication, productivity and commerce. The combination of RSS feeds, instant messaging, e-mail and the Web has created new markets and opportunities for businesses of all sizes and across all vertical markets. Unfortunately, the criminal element and unscrupulous businesses are exploiting these avenues and seeking to monopolize these growing opportunities and technologies by stealing personally identifiable information and corporate data. As a result, ISPs and all receiving networks are faced with the onslaught of increasing volumes of spam and malicious e-mail. While content filters and heuristics were effective counter measures against traditional spam and content chaff, image based spam, bots zombies and phishing exploits force significant changes to protect users and their personal information.

In today's environment where daily vigilance against emerging threats is needed, even a sender with impeccable practices, Sender ID authentication, relevant content, and the expected frequency may see fluctuations in deliverability. For example, when a large virus outbreak hits, the biggest mail servers with the most users are affected the worst. This can result in billions of additional messages and significant increased load on mail servers. As mail servers get overloaded, available incoming SMTP connections can get tied up and spam filtering engines fall behind. Mail servers eventually can slow or stop accepting new connections while they process the connections they have open. From a sender's perspective, it can be hard to know if your connection is being rejected due o a poor reputation or because of an exploit hitting a specific receiving network or the ecosystem at large.

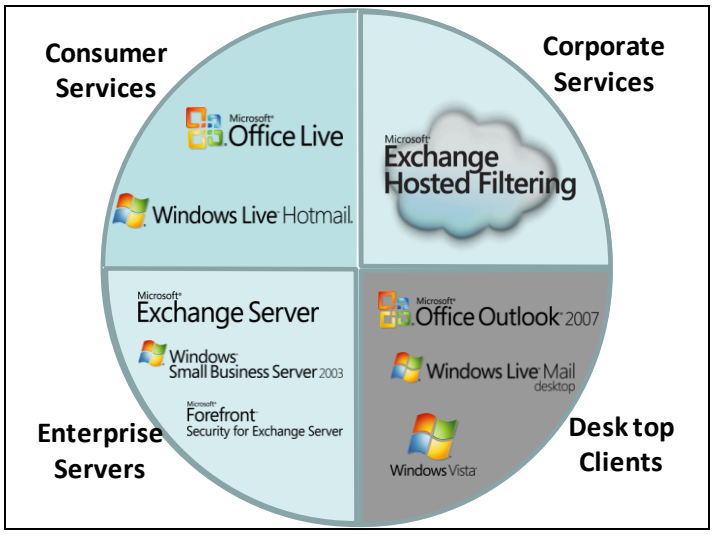
In another scenario, consider that every day receiving networks may deploy new solutions and enhancements in the fight against spam, viruses and phishing. As each update is made, the behavior of the overall system may change. These changes can impact deliverability for some senders and not for others, or at only certain times. It would be impractical and somewhat self defeating to publish a schedule of such countermeasures. Yet from a sender's perspective, not having any insight into can negatively impact.

Marketers and advertisers who understand the way the pieces fit together can optimize their delivery and yield a competitive advantage over those who do not pay. Those who send messages in the gray area between best practices and poor practices will have the more challenges than those who are constantly monitoring and improving their practices. This whitepaper attempts to provide insights into best practices and recommendations to aid in the deliverability of legitimate e-mail while enhancing end-user trust and confidence.

Microsoft Anti-Spam Overview

Meeting a diverse range of user needs and environments, Microsoft has developed several e-mail products and services, being used by hundreds of millions of users worldwide. Combined, this has created the largest ecosystem of e-mail servers, services and clients in the world, providing enhanced layered protection against spam, phishing and viruses. Through feedback and daily user analysis, Microsoft continues to invest in protection, proof and prevention technologies, helping customers maximize their trust, confidence and productivity in e-mail and all forms of electronic messaging.

- Microsoft Office Outlook 2003 & 2007
- Microsoft Exchange Server 2003 Intelligent Message Filter
- Microsoft Exchange Server 2007 with Microsoft Forefront Security for Exchange Server
- Microsoft Exchange Hosted Filtering
- Windows Mail (Windows Vista) and Windows Live Mail Desktop Client
- Windows Live Hotmail / MSN Hotmail
- Entourage Client for MAC



Microsoft's Online Safety & Security Strategy including anti-spam and anti-phishing incorporates a holistic approach including three primary disciplines, (for more information visit www.microsoft.com/safety):

1. Prescriptive Guidance - Providing user and business with tools and resources.
2. Collaboration - Commitment to Industry, Government and Business Collaboration including industry working groups, partnerships, legislation, standards and policies
3. Technologies Investments - ecosystem of servers, services and clients:
    a. Sender Reputation
        i. IP, URL, domain and user reputation
        ii. Attack detection
    b. Authentication + Identity
        i. Sender ID Framework
        ii. Outlook Email Postmark
    c. Content Filtering
        i. Low cost machine learning algorithm (user driven)
    d. User Personalization
        i. Direct and indirect user behavior and feedback
        ii. Graymail, e-mail that is desired by some and not others

As part of Microsoft's commitment to online safety and protecting the e-mail ecosystem, Windows Live Hotmail has made the following investments with the mutual goals of protecting users from deceptive and unwanted e-mail, reducing Spam in the Inbox (SITI), reducing operational impact while improving the deliverability of legitimate e-mail. Receiving feedback from millions of end-users Microsoft has developed the new Windows Live Platform including;

- New Safety UI to help warn and protect users from spoofed or phishing e-mails
- IP Throttling and block lists to reduce overall volume
- Integration of the Sender ID Framework, authenticating inbound and outbound e-mail
- Junk e-Mail Reporting Program (JMR)
- Smart Network Data Services (SNDS)

We continue to improve deliverability for legitimate senders by improving IP and volume based reputation data. At Hotmail, the Sender ID verdict result is combined with pre-existing reputation data to determine an enhanced e-mail "trustworthy score". Computation proofs, such as the Outlook 2007 Postmark, help end-user systems distinguish between legitimate mail and spam, reducing the incidence of false positives and enhancing their individual mail deliverability. Offering a safe and secure unsubscribe option has helped reduce the number of user complaints, providing senders enhanced data for list management , while not adversely impacting their overall reputation[1].

Looking ahead, Microsoft will continue to research and invest in reputation and authentication technologies. Conceptually servers, services and clients will share central reputation data. Multiple levels of reputation will be tracked including IP, URL, domain and use. The Sender ID Framework and the Outlook Postmark will help authenticate users and create identities. Finally, user personalization elements will be integrated as we continue to learn from user to better distinguish good e-mail from bad e-mail.

Summary of Deliverability Best Practices

Specific to Windows Live Hotmail, we highly recommending following these steps to ensure the highest deliverability rates:

Step 1 - Ensure Compliance -With Windows Live Policies and Technical Requirements

- http://postmaster.live.com/Guidelines.aspx

Step 2 - Follow best practices and FAQ's

- http://postmaster.live.com/Troubleshooting.aspx
- http://www.microsoft.com/postmaster

Step 3 - Adopt Sender ID and Keep Your Record Current

- http://www.microsoft.com/safety
- http://www.microsoft.com/SenderID

Step 4 – Join the Junk e-Mail Reporting Program

- http://support.msn.com/default.aspx?productkey=edfsJMRp&mkt=en-us

Step 5 – Leverage Smart Network Data Services (SNDS)

- https://postmaster.live.com/snds/index.aspx

Step 6 – Contact Deliverability Support - If you're still having issues: http://support.msn.com/eform.aspx?productKey=edfsmsbl&page=support_home_options_form_byemail&ct=eformts

[1] In the future Senders who realize an excessive number of unsubscribe requests may have their reputation impacted.

Consistent and reliable e-mail deliverability generally comes down being consistent, monitoring your reputation proactively and following best practices. The following tenets and their impact to deliverability should be considered by all senders and online marketers:

1. **Complaints** - This occurs automatically when a user clicks “block and delete”, “report spam” or similar reporting options including escalations and user complaints. This might be the complaint rate or just the total number of complaints depending on the receiver.

2. **High unknown user rates** - How clean is your list? Are you sending mail to users that have moved on and changed address? Do you have a lot of dead addresses on your list? This is an indicator by many receivers that you may be a spammer and indicator of harvested address lists.

3. **Spam trap addresses** - These are addresses (in some cases a domain) that have never been signed up to receive any kind of message or have been deactivated after prolonged inactivity by the ISP. Typically ISPs and law enforcement agencies create these and post them on web sites to be “harvested”.

4. **Sending infrastructure** - Spammers steal resources and have difficulty setting up “industrial strength” infrastructure. Many receivers look for well set up infrastructure as another indicator.

5. **Sending “permanence” (Consistency**) – Sending from the same IP address with consistent volumes and frequencies month over month is ideal. Spammers tend to “pop up” on an IP and disappear. Infrequent senders who send large volumes once a month or quarterly can be an indicator of a spammer or a compromised server.

6. **Content** – Senders be focused on e-mail content, as well as the URLs and HTML elements embedded in their e-mail. Anti-spam systems and heuristics continue to incorporate content filtering with authentication and reputation for a combined “trustworthy” score. Reputation scoring can compensate for content which may appear “spammy”, resulting in improved deliverability and a reduction in false positives.

The following sender best practices may help increase your chances for successful deliverability:

Complaints

- Add “list unsubscribe” header to e-mails offering subscribers a clean way to opt out
- Honor unsubscribes requests. Opting out should be just as simple as opting in
- Add text reminding subscribers where they opted-in to receive your e-mail
- Monitor your complaint rates. Most major services or e-mail service providers offer monitoring tools for free or as part of their service.
- Validate you are adhering to applicable anti-spam and privacy laws and policies
- Ensure your marketing communications are timely, relevant, have been requested and that you have permission to send them to the user.
- Consider the frequency of your mailings. What are the user’s expectations?

High unknown user rates

- Maintain your mailing lists. This includes purging old, bad or inactive addresses from your mailing lists. Also, this means acquiring names responsibly and sending mail only to users that “opt-in” to receiving your e-mail.

Spam trap addresses

- Monitor and manage both hard and soft bounces. Bounce notices can provide invaluable information regarding the ISP's treatment of your e-mail.

Sending infrastructure

- Choose content wisely and verify URLs look normal and point to valid domains
- Format a reply header to ensure subscribers see your "friendly" e-mail address
- Use a reputable e-mail service provider who has relationships with ISPs, such as AOL, Yahoo and Windows Live Hotmail
- Implement outbound e-mail authentication using the Sender ID Framework, with a valid "-all" record. This helps protect from spoofing and ensure your MTA is authorized to send mail, while protecting the brand and domain from threats to their brand and misrepresentation.
- Segment or separate traffic by brand or type of mail. Corporate e-mail, customer acquisition, customer retention and transactional e-mails should be segmented. Senders who wish to maintain separate reputations for each should consider segment mail streams by IP address and publishing separate SPF records.
- Set up, monitor and proactively manage your user feedback data. Feedback loops contain valuable spam complaint information

Sending "permanence"

- Be consistent – Send e-mail from the same IP's
- Less is more. Send less mail more often vs. lots of mail for short periods of time

The bottom line to remember is: if as little as 1% of your customers complain, the inability to communicate with your entire customer base may be the end result.

Finally, before launching any campaign, thorough testing is recommended. This means frequent testing with recipient accounts using various clients and major e-mail service providers to ensure that communications are being received in a desired fashion.

Deliverability Scenarios

Scenario 1: Your e-mail is being delivered to the Junk e-mail Folder

Symptoms
1. Open, click and unsubscribe rates decline
2. Recipients inform you that your e-mail is delivered to the JMF
3. Some or all of the e-mail sent to your personal Windows Live Hotmail account is delivered to the Junk e-mail Folder (JMF).

Common Causes	Recommended Actions
Too many recipients reported your previous e-mails as spam	✓ Change the Subject lines of your messages to be more relevant ✓ Make sure the From address is recognizable and would never be perceived as deceptive ✓ Reduce the frequency of your messages ✓ Make sure you are sending what the recipients expect to receive ✓ Increase the relevance of your messages ✓ Reduce frequency to addresses that have not opened or clicked recently ✓ Make the Unsubscribe option easy to find and use ✓ Include a List-Unsubscribe header ✓ Send an immediate confirmation message ✓ Add more relevant text content to your messages ✓ Sign up for the Smart Network Data Services (SNDS) service from http://postmaster.live.com for a daily view of your complaint rates. ✓ Sign up for the Junk e-Mail Reporting Program (JMR) to receive junk e-mail complaints reported by customers for your IP addresses. For more details, see http://postmaster.live.com.
Too much of your mail is sent to invalid or inactive e-mail addresses	✓ Avoid mailing addresses that have not responded to your mail (i.e. opened or clicked) recently, or from users that have requested to be unsubscribed ✓ Ensure that addresses that receive NDRs or bounce more than 2X are removed ✓ Sign up for the Smart Network Data Services (SNDS) service from http://postmaster.live.com for a daily view of delivery attempts to our Dynamic Trap Accounts - DTA's.
Your Sender ID record is incorrect or missing	✓ Insure your outbound mail is Sender ID compliant by publishing an SPF record in your DNS and that your IP's and related domain records are current

Scenario 2: Your is delivered successfully via SMTP without a bounce but not delivered to the Inbox or JMF

Symptoms
1. Open, click and unsubscribe rates decline
2. Recipients inform you that your e-mail is not delivered to the Inbox or the JMF
3. Some or all of the e-mail sent to your personal Windows Live Hotmail account is never delivered to the Inbox or the JMF

Common Causes	Recommended Actions
You are sending to Symantec Brightmail™ dynamic spam/trap accounts or Windows Live Hotmail Dynamic Trap Accounts	✓ Reduce frequency to addresses that have not opened or clicked recently ✓ Ensure that addresses that receive NDRs or bounce more than 2X are removed ✓ Segment mailings (transactions, newsletters) by IP address and try to identify bad data segments or sources.
Too many of your e-mail messages have been detected as SPAM by our internal filtering and reputation systems	✓ Change the Subject lines of your messages to be more relevant ✓ Make sure the From address is recognizable and would never be perceived as deceptive ✓ Reduce the frequency of your messages ✓ Make sure you are sending what the recipients expect to receive ✓ Increase the relevance of your messages ✓ Reduce frequency to addresses that have not opened or clicked recently ✓ Make the Unsubscribe option easy to find and use ✓ Include a List-Unsubscribe header ✓ Send an immediate confirmation message ✓ Add more relevant text content to your messages ✓ Sign up for the Smart Network Data Services (SNDS) service from http://postmaster.live.com for a daily view of Windows Live Hotmail how e-mail from your IP's are viewed by our systems and your recipients. ✓ Sign up for the Junk e-Mail Reporting Program (JMR) to receive the junk e-mail complaints reported by customers for your IP addresses. For more details, see http://postmaster.live.com.

Scenario 3: Your SMTP connections are blocked or mail is bouncing

Symptoms
1. You receive an unusually high number of bounce messages
2. Open, click and unsubscribe rates decline significantly
3. Recipients inform you that your e-mail is not delivered to the Inbox or the JMF
4. Some or all of the e-mail sent to your personal Windows Live Hotmail account is never delivered to the Inbox or the JMF
5. Your SMTP servers can't connect to Windows Live Hotmail

Common Causes	Recommended Actions
Server Configuration	✓ Properly configure anti-virus software on your firewall or your SMTP gateway ✓ Configure your Domain Name Server ("DNS") server correctly ✓ Enable Reverse DNS Lookup ✓ Ensure your outbound mail is Sender ID compliant by publishing an SPF record in your DNS ✓ Only send mail from a dedicated/static IP – Windows Live Hotmail doesn't accept connections from dynamic IP's
Microsoft Blocklist	✓ Please visit http://www.senderbase.org, http://www.kloth.net/services/dnsbl.php or http://openrbl.org to verify that your IP is not being targeted by any 3rd party block lists. ✓ If you believe your e-mail has been blocked in error by Microsoft, please review our best practices and technical guidelines to ensure compliance. ✓ For Windows Live Hotmail, please visit http://postmaster.live.com. Still having issues, contact our dedicated deliverability support team. Instructions can be found at http://www.microsoft.com/postmaster (or) http://postmaster.live.com/Troubleshooting.aspx
Volume Caps	✓ Utilize additional IP addresses within the same Sender ID record. ✓ Sign up for the Smart Network Data Services (SNDS) service from http://postmaster.live.com. This program allows a sender to monitor the 'health' and reputation of their IPs.

Contact and Escalation Procedures

Microsoft Monitoring Services: JMR and Smart Network Data Services (SNDS)

Contact Info: http://postmaster.live.com
Requirements:
For JMR: http://postmaster.live.com/Services.aspx#JMRP
For SNDS: http://postmaster.live.com/snds/

Microsoft Support to troubleshoot delivery issues
Requirements:
Answers to questions posted at:
http://postmaster.live.com/Troubleshooting.aspx

Sender ID
Inquiries on correct SPF record syntax and to help assure your records are included in the Window Live Hotmail SIDF cache e-mail senderid@microsoft.com, listing the domains you have published records for. Please allow for 48 hours after posting your record to the DNS for server replication. More information is available at www.microsoft.com/senderid

Third Party E-mail Delivery Consulting Services
Services are available from a broad set of third party service providers who provide e-mail marketing, deliverability and reputation enhancement services. For more information visit www.microsoft.com/postmaster, www.espcoalition.org/ and or www.authentication.org.[2]

Return Path's Sender Score Certified Program

Contact Info: http://www.senderscorecertified.com/register/
Requirements:
Senders must meet Program Standards, http://www.senderscorecertified.com/info_center.html.

[2] Listing is for information purposes and not endorsed by Microsoft. Companies should review service provider's capabilities and references.

Frequently Asked Questions

General

Microsoft and Windows Live Hotmail are committed to helping protect e-mail as an essential communications tool and to help protect users worldwide from spam, phishing and other e-mail safety threats. We firmly believe that using a mix of e-mail authentication including Sender ID and reputation can help ensure only legitimate e-mail is allowed to reach Windows Live Hotmail customers. All of the systems and processes are designed to help separate legitimate e-mail from unwanted mass marketing e-mail, helping senders and receivers communicate more effectively over the Internet.

Through a combination of layered e-mail filtering, heuristics, authentication and reputation services, we help block more than 95% of incoming spam from reaching MSN Hotmail and Windows Live Hotmail users' inboxes. This translates into almost 4 billion spam messages blocked every day.

Q. What is Windows Live Hotmail doing to combat spam?
A: Microsoft has made a serious commitment to work alongside industry and government to fight spam on many fronts. We believe it will take a combination of advanced technology, industry self-regulation, consumer education, effective legislation and targeted enforcement against illegal spammers to significantly reduce and solve the spam problem.

- Sender ID Framework (SIDF) is providing significant protection for consumer and business value. Today SIDF has been adopted by over 9 million domains and over 43% of all e-mail sent daily. SIDF is improving the deliverability of legitimate e-mail while dramatically reducing false positives and false negatives, providing user increased confidence and trust in their e-mail in their inbox, while reducing the risk of spoofing, phishing and deception.
- We're swiftly delivering cutting-edge innovations to help customers. We're continually improving these technologies, such as our SmartScreen™ filter, which trains itself by incorporating the feedback of Windows Live Hotmail users.
- We are working with others in the industry to promote standards and best practices that will help identify legitimate mail so filters can focus harder on stopping spam. Microsoft is on the boards of many industry and business organizations including the Anti-Phishing Working Group (APWG), Authentication and Online Trust Alliance (AOTA), Direct Marketing Association (DMA) and the Messaging Anti-Abuse Working Group (MAAWG).
- We're partnering with industry and governments to increase the risk and reduce the incentive of spammers around the world through legal and policy avenues.

Q: What back-end features are in place in Windows Live Hotmail to help protect users?
A: Building a safer web mail experience remains a priority for Microsoft with Windows Live Hotmail and you can expect us to continue investing in this space. Some of the key checks we go through today to help protect customers from spam and phishing scams include:

- **Content Filtering:** Windows Live Hotmail uses Microsoft SmartScreen spam-filtering technology, which uses a machine-learning approach to not only help protect a customer's own inbox from junk e-mail, but also help others who use web mail. SmartScreen content filter learns from known spam and phishing threats as well as from Windows Live Hotmail customers who have opted in to be part of the Feedback Loop program (FBL).

- **Sender ID verification:** The Sender ID Framework is an e-mail authentication technology protocol that helps address the problem of spoofing and phishing by verifying the domain name from which e-mail is sent. Sender ID validates the origin of e-mail by verifying the IP address of the sender against the purported owner of the sending domain.
- **Phishing heuristics-based check:** WLM analyzes embedded URLs against hundreds of thousands of common phishing Web site characteristics to help determine whether the e-mail might be dangerous. See http://www.microsoft.com/safety/antiphishing for more details.
- **Sender Score Certified:** Windows Live Hotmail currently utilizes the Sender Score Certified program to accredit, monitor and manage senders for use inclusion in WLH white list program.
- **User based Allow/Block list filtering (includes Allowed Mailing Lists check):** Customers can choose to receive mail only from individuals already set up in their Contacts or from specified domains that have been marked as safe or added to their allow list. This optional feature offers an even greater level of protection against unwanted e-mail. The blocked senders list allows Windows Live Hotmail customers to refuse e-mail from a specific sender.
- **Contact list check:** Based on your contact list.
- **SMTP Authentication check** (includes mails sent by MSN or Windows Live to Hotmail customers)

Q: How does SmartScreen™ work?
A: Microsoft Research's patented machine-learning technology SmartScreen™ spam and phishing filtering technology is applied across Microsoft's e-mail platforms to help provide customers with the latest anti-spam and anti-phishing tools and innovations.

SmartScreen learns from data provided regarding known phishing threats as well as from Hotmail and Windows Live Hotmail customers who have opted in to provide input to determine what characterizes good mail and unwelcome mail (such as spam and phishing scams). Machine learning includes probability-based algorithms used to distinguish between legitimate e-mail and spam training on the characteristics of both types of e-mail.

SmartScreen data from Windows Live Hotmail users has been integrated into the latest versions of e-mail products and services, including Windows Live Hotmail, Exchange Server 2003/2007, Outlook 2003/2007, Outlook Express and others.

Q: Does Windows Live Hotmail use Symantec Brightmail™?
A: In addition to SmartScreen, incoming e-mail is evaluated by Symantec's Brightmail anti-spam content filter. Leveraging the "Probe Network", a collection of more than two hundred thousand (200,000) e-mail addresses designed to attract junk e-mail; Symantec's patented technology identifies and eliminates junk e-mail before it reaches a Windows Live Hotmail user's inbox. Symantec's proven solution provides protection against unsolicited junk e-mail by offering a dynamic technology that keeps pace with constantly evolving junk e-mail. To learn more about this technology, please visit http://www.symantec.com.

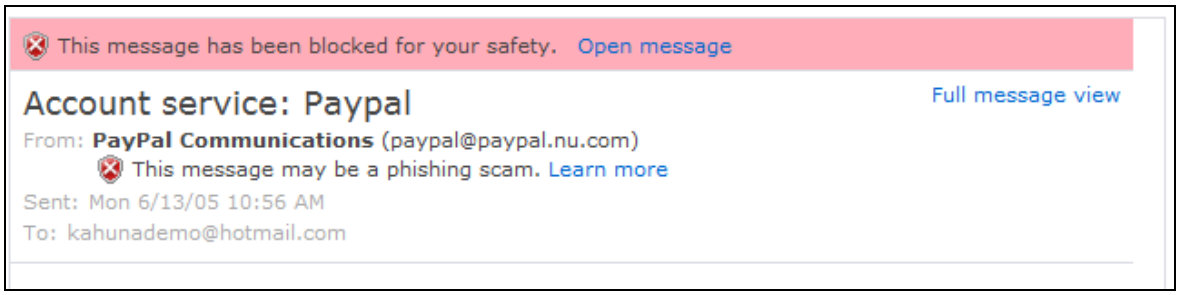
Q: Does Windows Live Hotmail use Sender Score Certified from ReturnPath?
A: Yes, One of Windows Live Hotmail's solutions to help address and mitigate false positives and enhanced deliverability is the Sender Score Certified program. This program identifies e-mail based on their past sending behavior and their adherence to strict program standards.

To qualify participants must meet a set of practices and are required to maintain high quality e-mail programs with low complaint rates in order to remain in the program. Participation helps avoid false positives but does not guarantee delivery; Microsoft's terms of use and guidelines must still be honored. For more information, visit www.senderscorecertified.com.

Q: Can Hotmail and Windows Live Hotmail users create their own filter settings?
A: In addition to the anti-spam filtering technologies, Windows Live Hotmail (as well as Outlook) enables each user the ability to set filter levels to further improve the delivery of e-mail and block undesired e-mail to their account. Users can easily add a sender or domain name to the Allowed Sender List so that e-mail from that sender or domain is never treated as junk e-mail regardless of the content of the message. Users can configure the settings to accept only messages from Contacts and Safe Senders List, giving total control over which messages are received. E-mail messages from a certain e-mail address or domain name can also easily be blocked by adding the sender to a user's Blocked Senders List. In addition, each time a message is reported as junk e-mail, using the "report and delete" or the "Unsubscribe" functions, messages from those senders e-mail address or domains are automatically added to a user's Blocked Senders List. Once a user adds a sender to their personal Block Senders List, e-mail from that sender will always be treated as junk e-mail from that point on, regardless of the content of the message. For more information, please visit http://www.microsoft.com/presspass/features/2003/nov03/11-17spamfilter.asp.

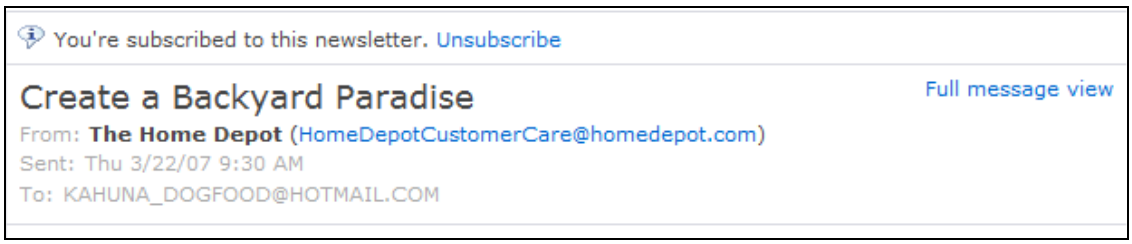
Q: Why are images and links disabled in some messages?
A: After extensive research and usability testing, the Windows Live Hotmail Safety Bar has been developed to help the user quickly distinguish between legitimate and desired e-mail vs. deceptive, malicious or undesired e-mail. I n the user experience, the analogy we use is that of the stop light. Unknown and suspicious mails are giving yellow or red treatment depending on how the e-mail is scored. As we expand the deployment of Windows Live Hotmail worldwide we expect the Safety Bar and user experience to evolve.

- Red: This means that the sender has failed Sender ID or that certain qualities of the message have identified it as a potential phishing exploit.



- Yellow: Indicates the sender is not in the safe list or the contact list. However, even if a sender is in your contacts/safe list you may see a yellow/red bar if the message fails or is not authenticated by Sender ID and other checks

- Known senders: Known senders have no safety bar messaging and the full contents of the mail are displayed. For known senders who have included the Unsubscribe header in their e-mail header, users are presented with the “unsubscribe” option as illustrated below.



Q: If my message displays properly in Hotmail, will it look the same in Outlook?
A: No, we recommend that messages be tested with both Outlook 2003 and 2007 as well as Hotmail as messages may not be rendered the same way in all e-mail clients and services. Outlook 2007 no longer support style sheets the same way previous versions of Outlook did. This means that even if HTML content looks fine in Internet Explorer and Outlook 2003, it may not in Outlook 2007.

Here are a few recommendations for improving Outlook rendering:

- **Do not use background images.** Background images, whether specified in the <body>, <table>, or <td> tag, cannot be used because of inconsistencies among e-mail clients, most notably Outlook 2007.

- **Do not use CSS (cascading style sheets), inline styles or JavaScript.** Cascading style sheets, where the styles are defined within the Web page itself, are only fully supported in most e-mail clients. Attached style sheets are not supported at all. Additionally, Web e-mail clients such as AOL Webmail and Gmail change or comment out style tags, resulting in unpredictable formatting. As a result, we recommend that you use only basic HTML tags. (For instance, to underline text, use the <u> tag, for bold use the <b> tag.)

- **Inline style attributes are your only option.** Use only the most basic style attributes to designate font size, color, and type, and use them within basic HTML tags (do not use or tags). Do not use styles to set table or row heights or any spacing. Do not define your style elements within the <head> tag of the document (Hotmail will entirely strip this out). JavaScript is not supported in any e-mail client. Do not include any JavaScript, including onClick=”return(false);” in your HTML.

- **Set table width to 600 pixels max.** The convention for HTML e-mail is to limit a set table width to 600 pixels. Though a wider table may render fine in Outlook or on a high resolution monitor, users with older systems or who choose an 800 X 600 display setting will not be able see the entire width of the e-mail.

- **Do not use the <body> tag to set any essential attributes.** Some Web e-mail clients (notably Yahoo and Hotmail) strip out the BODY tag within e-mails completely. You should not include any attributes in the BODY tag. To set values such as background color, use the BGCOLOR attribute inside the TABLE or TD tags.

- **Use HTML character names.** Many e-mail clients won’t display raw 8-bit characters correctly (they’ll show up as question marks or squares instead). As a result, you must use HTML codes for these characters. Use only the HTML names, not the numeric values.

- **Put image maps inside <body> tags.** When using image maps, the <MAP> and <AREA> tags should be between the open and close <BODY> tags with the rest of the content. The links will not work in certain Web e-mail clients that strip out everything above the <BODY> tag (such as Hotmail).

Additional information on Outlook can be found at the following:
- Outlook 2007 HTML capabilities http://msdn2.microsoft.com/en-us/library/aa338201.aspx
- Outlook 2007 Content Compatibility Tool http://www.microsoft.com/downloads/details.aspx?familyid=0b764c08-0f86-431e-8bd5-ef0e9ce26a3a&displaylang=en

Server Configuration

Q: What are the recommended SMTP connection settings for Windows Live Hotmail?
A: Windows Live Hotmail allow up to five hundred (500) concurrent connections from a single IP address, but each message is limited to one hundred (100) recipients. This is threshold dictated by the following RFC: http://www.faqs.org/rfcs/rfc821.html.

Q: Is there a maximum number of messages that can be sent from a single IP address?
A: Every IP address has a volume cap depending on its sending reputation. New IP addresses with no reputation are limited to thousands of messages per day. Established IP addresses with a good reputation and history of sending a high volume of messages are limited to 3-4 million e-mail messages per day. This number could change without notice and is updated frequently.

Q: What is the best way to introduce new IP addresses?
A: If you are adding new IP addresses, you should include them in your existing Sender ID SPF record so that they can benefit from your existing reputation. New IP addresses added to an existing Sender ID record enjoy the same reputation and volume caps as the IP addresses already referenced by the Sender ID record.

Q: How should I configure my anti-virus solution on my firewall or SMTP Server?
Some deliverability issues are the result of sender-based software configurations. If you are running anti-virus software on your firewall or SMTP server, check for a setting such as “Internet E-mail Auto Protect” or “Internet E-mail Protection.” If this setting is enabled, please disable it and try sending a test message again. If you are running Symantec Anti-Virus Corporate Edition 9.x, please review the following article from Symantec: http://www.symantec.com/enterprise/support/

Q: How can I confirm that my DNS is set up correctly?
A: Try connecting to mail.hotmail.com via port 25. If you are unable to connect to mail.hotmail.com, try telneting over port 25 directly to the Windows Live Mail e-mail servers (MTAs). You can find the current list of MTAs by querying “nslookup – q=mx hotmail.com” from a command prompt (this action should work on a variety of operating systems). Currently, the addresses for these servers are mx1.hotmail.com, mx2.hotmail.com, mx3.hotmail.com, mx4.hotmail.com. If that does not work, try connecting directly to the IP’s. If you are able to connect directly to the IP and not mail.hotmail.com this probably means there is a problem with your DNS server.

Occasionally, some of the IP’s in the MX record may be out of service. If you are connecting to one of these IP’s your connection may timeout. For your tests, you should make sure you test all of our published IP’s. In addition, you should configure your outbound e-mail server to do a round-robin DNS lookup for hotmail.com.

Q: How important is Reverse DNS?
A: Windows Live Hotmail may not accept e-mail from senders who fail a reverse-DNS lookup. In some cases legitimate senders advertise themselves incorrectly as a non- internet routable IP when attempting to open a connection to Windows Live Hotmail. IP addresses that are reserved for private (non-routable) networking are 192.168.0.0/16, 10.0.0.0/8, and 172.16.0.0/11 (or 192.168.0.0 - 192.168.255.255, 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255). The most common private network is 192.168.0.0.

Q: What is the Sender ID Framework (SIDF)
A: Sender ID is: a cost and resource effective authentication technology that has been adopted by over 9 million domains world-wide. The business and technical value and ROI has been validated by Windows Live Hotmail and various other receiving networks to significantly increase spam detection by 7-9%, and when combined with reputation data reduces false positives by over 85% when compared to similar senders who have not adopted.

Developed in concert with many industry leading include AOL and Sendmail, SIDF is an easy to deploy server-based, no cost solution offering ease of maintenance with no user interaction or client software changes required. SIDF has been designed to verify that each e-mail message originates from the Internet domain from which it claims to come based on the sender's SMTP server IP address. Eliminating domain spoofing will help legitimate senders protect their domain names and reputation, and help recipients more effectively identify and filter junk e-mail and phishing frauds.

Sender ID when checking via the Purported Responsible Address (PRA) helps prevent and blocks phishing and spoofing schemes by verifying the IP address of the e-mail sender against the reported owner of the sending domain. Spoofing attacks refer to domain spoofing which is the use of someone else's domain name when sending an e-mail, and is part of the larger problem of spoofing (the practice of forging the sender's address on e-mail messages). Domain spoofing can also be used by malicious individuals in phishing frauds, which try to lure consumers into divulging sensitive personal information by pretending the e-mail is from a trusted source, such as a financial institution or online service. Disclosure of such information can lead to identity theft and other online consumer fraud.

To learn more, please visit http://www.microsoft.com/senderid. To assist domain holders and mailers, Microsoft has created a simple wizard to create your SPF record for DNS posting. For more information visit www.microsoft.com/senderid/wizard.

Unsubscribe

With the launch of Windows Live Hotmail, we are committed to helping protect our customers from unwanted e-mail and continually evolve our approach to better empower our customers to take control of their inboxes. As a part of this effort, we provide options for customers to provide direction on how their e-mail is to be handled, such as Marking a sender as “Safe” or “Unsafe”, telling the Windows Live Hotmail service to deliver mail from senders they want to hear from, and reporting mail as “Junk” to report and block future e-mail from a specific sender.

In this vein, we also recently introduced a new option for customers to easily and confidently unsubscribe from legitimate mailing lists when they wish to do so. By providing this new “Unsubscribe” option directly in the Windows Live Hotmail user experience, we are aiming to help users better manage their inboxes while providing legitimate senders important information to help better manage their e-mail lists to ensure they are only sending e-mail to people that want it. Providing an “Unsubscribe” option also ensures that we report more accurate data to our own junk e-mail filters, differentiating true “Junk” e-mail from mail simply no longer want to receive.

Q: How does this new unsubscribe feature work? I’m a legitimate sender and I’d like to get these unsubscribe notifications from Windows Live Hotmail.
A: If legitimate senders wish to allow Windows Live Hotmail customers to unsubscribe through their mail inbox, they should publish the e-mail or web-based “list unsubscribe” information in the list unsubscribe header (as specified in RFC 2369). Then, as long as the receiving Windows Live Hotmail customer has previously identified that sender as legitimate by marking the sender as “safe” or placing the address in their contact list, both functions add the sender to their personal “safe list”, the "unsubscribe" option will be available should the customer choose to unsubscribe at any time. The unsubscribe option is currently enabled for senders that participate in Return Path’s Sender Score Certified safelist program.

To unsubscribe, a user simply clicks the link when they see the text “You’re subscribed to this newsletter. Unsubscribe” This is shown at the top of the email message, and once clicked will attempt to remove the user from the mailing list as well as block future email from that address. By doing so, a user notifies the sender that they wish to unsubscribe from the mailing lists, and the e-mail message is not marked as “junk” helping to maintain the sender’s reputation.

Q: What if we only provide web based unsubscribe? Can those mail lists be unsubscribed to in this manner?
A: Yes, both the Mailto and URL unsubscribe (as outlined in RFC 2369) are supported in the Full version of Windows Live Hotmail. Currently only the Mail o option is supported in the Windows Live Hotmail Classic version, but the URL option in the future.

Q: I thought people weren't supposed to unsubscribe to any mail anymore, in case it was just an attempt from spammers to confirm active e-mail accounts?
A: In the past, consumers were often instructed to not to unsubscribe to unwanted mail, because it was hard to tell legitimate senders from deceptive mailers that might abuse the unsubscribe request. However, users often find they have opted-in for legitimate e-mail, and then later decide they want to opt-out. By making a distinction between a legitimate unsubscribe requests and a "junk" e-mail report, the Windows Live Hotmail anti-spam technology will improve the chance of other users receiving e-mail they want from the same sender. We are taking this step to try to help provide a trusted unsubscribe capability to our customers, but with fewer risks than clicking the unsubscribe link found within the e-mail message.

Because the unsubscribe option via Windows Live Hotmail is only available after a user has added the sender to their personal Safe List (which previously identifies that sender as legitimate), we believe this to be a safer way to unsubscribe to the legitimate e-mailers who want this information to help keep their e-mail lists 'clean', so they're only sending e-mail to people that actually want to hear from them. We believe this functionality will help improve e-mail senders' ability to maintain their mailing lists and respond to unsubscribe requests. By participating and taking steps to quickly clean their lists when they receive unsubscribe requests, legitimate mailers and e-marketers should be able to enhance their online reputation and the respective deliverability of their legitimate e-mail.

Q: What happens if I still continue to receive mail from a sender after I've unsubscribed?
A: Once a sender receives the unsubscribe request, it will take them some time to ensure that recipient's information is removed from their mailing lists. In many cases, this time is often regulated by law. However, Windows Live Hotmail also places the sender in the user's block list after clicking on Unsubscribe. Unless the sender uses a different email address from which they send email from, this ensures that even if the sender doesn't uphold their end of the unsubscribe bargain, our users won't receive mail from them anymore.

Q: Are you using the standardized approach from RFC 2369 for the unsubscribe notification process?
A: Yes. For more information, please visit http://www.ietf.org/rfc/rfc2369.txt or http://www.list-unsubscribe.com/.

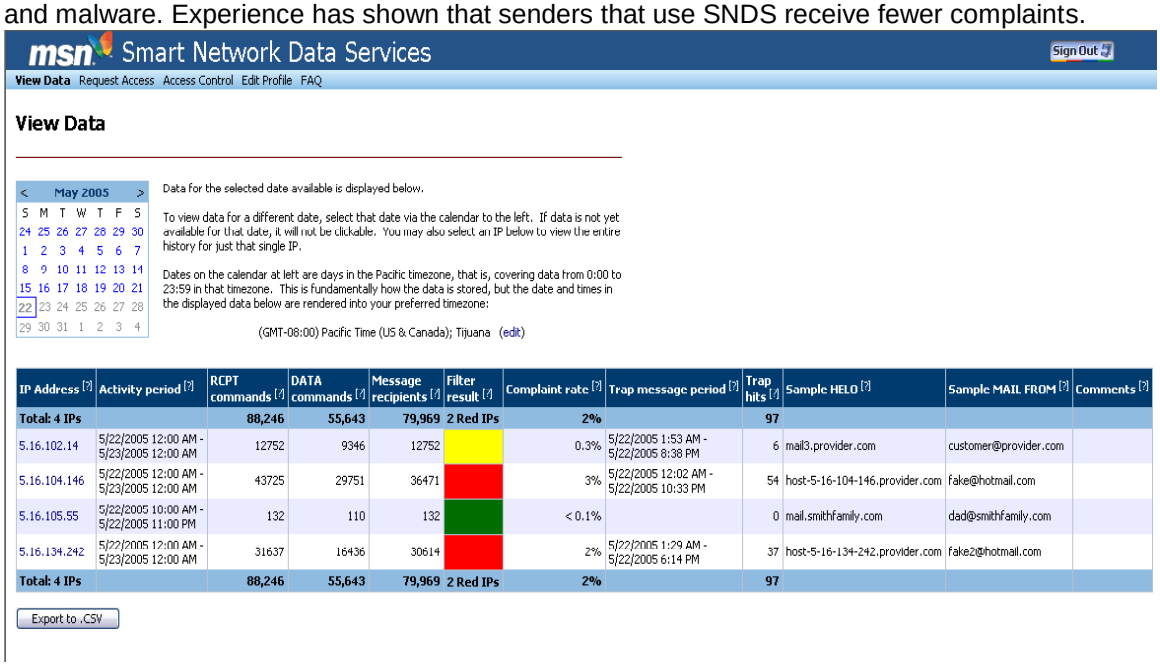
Q: I'm using MSN Hotmail/Exchange/Outlook/Outlook Express/Office Live Mail – can I do this too?
A: We continually evolve all our e-mail offerings as appropriate for each product or service environment to help put customers in greater control of their inboxes – but currently, this particular unsubscribe functionality is only available for users of Windows Live Hotmail.

Q: Are all ISPs providing this capability?
A: We are excited about taking this step as a positive way to help both our customers and the greater e-mail community, and hope to see other inbox providers providing similar capabilities to ultimately improve the trust and confidence in all forms of electronic messaging. We are working with industry working groups such as AOTA, ESPC and MAAWG to share information and best practices.

Sender Feedback – Smart Network Data Services (SNDS) and Junk e-Mail Reporting Program (JMR)

Q: What is Smart Network Data Services?
A: Smart Network Data Services (SNDS) is a web based service which provides visibility to service providers to track spam originating from within their IP space and data to empower senders to track their reputation.

Q: **What should I expect to see**?
Responsible parties can log in using an automated process to see detailed reports about unexpected or suspicious mail activity (from spammers, botnets, malware), mail volume received by Hotmail, user spam complaints, message attempts to invalid/dynamic trap accounts, viruses and malware. Experience has shown that senders that use SNDS receive fewer complaints.



Q: Where do I sign up for SNDS?
A: https://postmaster.live.com/snds

Q: Who is eligible to sign up for SNDS?
A: Anyone who can prove that they own an IP range is eligible to sign up for SNDS. Access to SNDS data can be delegated to third parties.

Q: Where can I find out more about SNDS?
A: https://postmaster.live.com/SNDS/faq.aspx

Q: What is JMR?
A: The Junk e-Mail Reporting Program (JMR) sends an e-mail notification to the sender of the message any time a MSN Hotmail or Windows Live or Hotmail user clicks the "Junk" button or "Mark as Unsafe". The sender can use this information to monitor how users respond to their e-mails and may use this to unsubscribe specific e-mail addresses.

Q: Where do I sign up for JMR?
A: http://postmaster.live.com/Services.aspx#JMRP

Q: Who is eligible to sign up for JMR?
A: Anyone is eligible to sign up for the JMR. However, we do have some criteria that the sender must meet: They must own their IPs or at least have exclusive sending rights and they must be able to remove the complaining e-mail addresses from their mailing lists.

Q: How are JMR notifications sent?
A: JMR forwards a copy of the original message anytime a Windows Live or Hotmail user clicks on the "Report and Delete" link.

Q: What does a JMR notification look like?
A: An example is included below:

Header

```
Return-Path: <staff@hotmail.com>
Received: from BAY0-JMR-SMTP02.phx.gbl (64.4.60.249) by mail17.domainname.com id h2lrrk0ab0ob for
<hotmailabuse@ domainname.com >; Thu, 5 Apr 2007 17:27:06 -0500 (envelope-from
<staff@hotmail.com>)
Received: from BAY0-JMR-DB01 ([10.1.194.126]) by BAY0-JMR-SMTP02.phx.gbl with Microsoft
SMTPSVC(5.0.2195.6713);
         Thu, 5 Apr 2007 15:27:00 -0700
From: staff@hotmail.com
To:  hotmailabuse@ domainname.com
Subject: complaint about message from 69.56.33.72
Mime-Version: 1.0
Content-type: multipart/mixed; boundary="=JMR_00a5_758cb5a2.f0f875b3"
Return-Path: staff@hotmail.com
Message-ID: <BAY0-JMR-SMTP02ItMc000057a1@BAY0-JMR-SMTP02.phx.gbl>
X-OriginalArrivalTime: 05 Apr 2007 22:27:00.0507 (UTC) FILETIME=[874B2EB0:01C777D1]
Date: 5 Apr 2007 15:27:00 -0700
```

Body

```
--=JMR_00a5_758cb5a2.f0f875b3
Content-Type: message/rfc822

X-HmXmrOriginalRecipient: carrie_critendonwraith@hotmail.com
X-Message-Status: n:0
X-SID-PRA: University Education <University@domainname.com >
X-SID-Result: Pass
X-Message-Info: tx435uGaQdmn7Z5JQSJmYXEJIe/LvSfipiBWlcuJGybO3Lw4LqHa+OVnc
Received: from mail24.domainname.com ([11.11.11.11]) by bay0-mc7-f5.bay0.hotmail.com with
Microsoft SMTPSVC(6.0.3790.2668);
         Sun, 1 Apr 2007 01:39:40 -0700
DKIM-Signature: a=rsa-sha1; c=relaxed/relaxed; q=dns; s=default; d= domainname.com;
 h=Message-ID:Date:From:To:Subject:Mime-Version:Content-Type;
 b=CHMC7LInguWtxru3IfIh0j6EQjSJ3Q6xgi7WgMLpSZJdhxhPMQ9VE5VVe4SmJ7KV2jbXxjA8igAT
   gTUCd+ALMQ==
DomainKey-Signature: a=rsa-sha1; c=nofws; q=dns; s=default; d= domainname.com;
 b=JJVlpT94E/jX59zQjYBHFBy5YxH86Jl/amvXj0HRDdyNbavHUe7R9/to0O1/WTwzTar+2PwAVUqm
   ztYzWSwUnQ==;
Received: by mail24. domainname.com.com id h1tntc0ab0oi for <johndoe@hotmail.com>; Sun, 1 Apr
2007 03:38:47 -0500 (envelope-from <bounce-piiipxgemxgxg@ domainname.com >)
Message-ID: <32329920.1175416703315.JavaMail.root@ domainname.com >
Date: Sun, 1 Apr 2007 03:38:23 -0500 (CDT)
From: University Education <University@ domainname.com >
Reply-To: Domain <xwwwczrbmzrzr@ domainname.com >
To: "carrie critendon" <carrie_critendonwraith@hotmail.com>
Subject: University Education!
Mime-Version: 1.0
Content-Type: multipart/alternative;
         boundary="----=_Part_9044_22182547.1175416703314"
X-exct: sxohhccxljndnjooondshlc nnbnllnxcyjccchdsnjdsds cobschbln
Return-Path: bounce-piiipxgemxgxg@excite-partners.com
```

Windows Live Sender Reputation Data

Q: What is Windows Live Sender Reputation Data?
A: Windows Live™ Hotmail and MSN® Hotmail services utilize Microsoft's patented SmartScreen anti-spam filtering technology. This technology uses a machine-learning approach to help protect users' inboxes from junk e-mail. SmartScreen technology learns from known spam and Phishing threats as well as from Windows Live Hotmail or MSN® Hotmail customers who have chosen to participate in the Feedback Loop Program (FBL). The FBL program differs from other Junk Mail Reporting programs since users are invited to participate. Throughout the year participants are cycled in and out, offering the ability to counter user fatigue and underreporting as experience in traditional JMR or FBL programs.

Windows Live Sender Reputation Data is a collection of non-biased responses from FBL participants over time. Along with other sources of reputation data such as the Junk e-Mail Reporting Program (JMR), the Windows Live Sender Reputation Data from FBL users helps to train and improve the way SmartScreen technology properly classifies messages based on e-mail content and sender reputation.

Q: How are participants selected for the program?
A: To ensure representative sampling across the e-mail user base:

- Participants for the program are selected at random for over 280 million active Windows Live users worldwide Uses cannot volunteer for this program
- Participants represent multiple languages and multiple types of services (i.e.MSN® Hotmail, MSN® premium, and Windows Live Hotmail).
- Participants are selected from the pool of subscribers who have an account that is active and at least 6 months old with users added and removed each month, providing objectivity and increase responsiveness from program participants.

Q: What is the current distribution of participants in this program?
A: Active feedback loop members herald from over 200 countries.

- 60% of feedback loop members use a non-English localized Windows Live Hotmail UI
- The average number of messages delivered to FBL users per day for classification typically varies between 200,000 and 300,000.
- Microsoft continually enlists new members and increases participation in the program.

Q: How do participants provide feedback about the e-mail they have received?
A: Random samplings of e-mail are extracted prior to any anti-spam technology which may subsequently filter out a particular piece of mail. This allows for the ability to learn from e-mail that otherwise may not have been delivered to the recipient.

Program participants are always presented e-mail for classification that was originally addressed to them. They are simply asked to classify the message as "not junk" or "junk". This is an important part of the program – users are only asked to comment on e-mail that was originally addressed to them, and they are never asked to comment on e-mail that was not addressed to them. Users must choose to classify the message either as "junk e-mail" or "not junk e-mail", and then are prompted to confirm their selection.

Q: How much does Windows Live Reputation Data determine if mail is "junk" status?
A: Reports from one FBL user cannot create junk status and requires additional feedback from other FBL users. Combining feedback from multiple FBL participants, along with other sources of reputation data, allows for junk or not-junk status to be applied.

Q: Is this data representative of all e-mail sent via Microsoft e-mail systems?
A: Yes, the program captures data for all senders delivering into MSN® Hotmail and Windows Live Hotmail.

Q: Isn't the program skewed toward participants who would want to only vote mail as Junk?
A: No. Participants are selected at random from over 200 countries without any bias or consideration for their previous voting record. Reports from one FBL user cannot create junk status and requires additional feedback from other FBL users. Combining feedback from multiple FBL users, along with other sources of reputation data, allows for junk or not-junk status to be applied.

Q: Is the sampling really random? Is there ever any intentional selection for a particular IP address or sending domain?
A: No. E-mail is selected for classification at random without any consideration of any particular sender, IP Address, or sending domain.

Q. How is participant feedback solicited on an on-going basis?
A. Once a user signs up to classify randomly selected messages, they periodically receive e-mail that has a subject of "Junk E-mail Classification". Users only classify e-mail originally addressed to them. E-mail is presented for classification within 12 to 24 hours of the messages original receipt for delivery to them. An example of a Classification E-Mail message is provided below.

Subject:	Junk e-mail classification
Body:	Thanks for helping us fight junk e-mail. Please look at the e-mail message below and tell us whether or not it's junk e-mail. If you're reading this message on the Web, it will be removed from your Inbox when you make a selection. <button>Not junk e-mail This is a message I'd expect to receive in my inbox. It's not junk e-mail. <button>Junk e-mail This is not a message I'd expect to receive. It's junk e-mail, and I'd like all similar messages to be blocked from my inbox. You're receiving this e-mail message because you volunteered to help us stop junk e-mail. If you've changed your mind, you can stop participating. This is an unmonitored e-mail address. If you're using MSN® Hotmail, you'll see a confirmation page each time you report junk e-mail. If you want, you can change this setting.

Q: Isn't the presentation in the message requesting classification biased?
A: No. Members are sent e-mail classification request for **e-mail that was addressed only to them**. Messages being classified may have been previously delivered to the inbox or intended to be delivered but either routed to the junk folder or deleted by the junk e-mail filter. Participants are then asked in a non-biased and objective manner how they would classify the message.

Additional Resources

For additional information, please visit the following Microsoft and industry resources:

Sender ID Framework: http://www.microsoft.com/senderid

Microsoft Windows Live Hotmail Postmaster Site: http://postmaster.live.com

Microsoft's Postmaster Site: http://www.microsoft.com/postmaster

Microsoft Windows Live Hotmail Guidelines: http://postmaster.live.com/Guidelines.aspx

Microsoft's Anti-Spam Policy: http://privacy.microsoft.com/en-us/anti-spam.aspx

Microsoft Safely Site: http://www.microsoft.com/safety

Microsoft Outlook: http://support.microsoft.com/kb/933793/en-us

Third Party Resources

FTC Guidelines for Businesses: http://www.ftc.gov/bcp/conline/edcams/spam/business.htm

Authentication and Online Trust Alliance (AOTA): www.aotalliance.org

Deliverability.com: http://www.deliverability.com/

Direct Marketing Association http://the-dma.org

E-mail Senders & Provider Coalition (ESPC): http://www.espcoalition.org

List-Unsubscribe.com: http://www.list-unsubscribe.com/

Managing the Age of Your User Lists: http://www.mail-abuse.com/an_listmgntgdlines.html

Messaging Anti-Abuse Working Group: http://www.maawg.org

Sender Score Certified Program: http://www.senderscorecertified.com.

Acknowledgements

Microsoft would like to thank the following organizations and individuals for their contributions to this paper; Joshua Baer from Datran Media, George Bilbrey from ReturnPath, the DMA, the Email Sender and Provide Coalition, (ESPC) and the Windows Live Hotmail product, development, support and planning teams.