Click to verify

Welcome Outlook.com Smart Network Data Services Deliverability to Outlook.com is based on your reputation. The Outlook.com Smart Network Data Services (SNDS) gives you the data you need to understand and improve your reputation at Outlook.com. But just looking at the data isn't enough! Maintaining a good reputation is a lot of work. You should use this data to keep your mailing lists clean and to monitor the IPs you control for unusual behavior. Reputation is always the responsibility of the sender. SNDS gives senders access to detailed data about individual IPs, and it also includes our Junk Email Reporting Program, which lets you receive reports when users junk your messages. Now you can view IP data and manage feedback loop settings from one convenient website. Getting started To access SNDS, please log in with a Microsoft Account and then request access to the IPs for which you are responsible. You'll be taken through a simple authorization process, and then you'll soon have access to a wealth of information about those IPs. Help! I have a problem sending mail to Outlook.com Building & maintaining good reputation is a long-term proposition. The data on this site can help you do that, but if you have an urgent deliverability issue please have the person most familiar with the issue and your email infrastructure contact sender support. Other Benefits SNDS is useful for far more than just monitoring email reputation. It can help IP owners to detect compromised servers, malware, viruses, and botnets. We help network administrators detect these problems so that they can clean them up and make the internet a safer place. Microsoft's email safety roadmap involves an unmatched cross-product approach. SmartScreen® anti-spam and anti-phishing filtering technology is being applied across Microsoft's email platforms to provide customers with the latest anti-spam and anti-phishing tools and innovations throughout the network. These products include Outlook.com, Exchange, Office 365, and more. The goal for Outlook.com is to offer a comprehensive and usable email service that helps detect and protect users from junk email, fraudulent email threats (phishing) and viruses. The Challenge Email has become an important communication tool not only for consumers but also for marketers, support staff, sales organizations, and businesses of all sizes. As email use has grown, so has email abuse. Unmonitored junk email can clog inboxes and networks, impact consumer satisfaction, and hamper the effectiveness of legitimate email communications. While technology alone cannot solve the problem, it is a critical component in our comprehensive anti-spam approach. That's why Microsoft continues to invest in research and development to advance anti-spam technologies. Simply put, it starts by containing and filtering junk email. Our Efforts We offer a number of steps to minimize the negative impact junk email has on our users' email experience. For example, we've implemented a number of mechanisms to reduce the burden of junk email which currently prevents nearly 4.5 billion email messages from reaching Outlook.com users every day! Junk Email Filters Microsoft SmartScreen® To help reduce the consequences of junk email, Outlook.com includes junk email protection using patented SmartScreen® technology which screens email to identify and separate junk email from legitimate email. Based on Microsoft Research's patented machine-learning technology, the SmartScreen® content filter learns from known spam and phishing threats, user feedback, as well as from Outlook.com users who have opted to be part of our junk email classification program. These types of data help train SmartScreen® how to recognize legitimate email and junk email and are key inputs into sender reputation. Machine learning refers to the probability-based algorithms that are used to distinguish between the different characteristics of legitimate and junk email. Ongoing feedback from Outlook.com customers in the junk email classification program helps ensure that the SmartScreen® technology is continually trained and improved. How does it work? When an external user sends email messages to an Outlook.com account, SmartScreen® filter technology evaluates the content of the messages and assigns the message a rating based on the probability that the message is junk email. This rating is stored as a message property called a spam confidence level (SCL) within the message itself. The SCL rating stays with the message as it is sent to other anti-spam protection layers within Outlook.com. Rules inside Outlook.com are set to handle email messages with various SCL ratings. If a message has an SCL rating lower than a certain threshold, it is considered spam and a rule then deletes the message rather than send the message to the users' junk email folders. If the message has a higher SCL rating than the threshold, the email is delivered to the user's junk email folder rather than to the inbox. Outlook.com Filters In addition to the anti-spam filtering technologies, Outlook.com also gives each user the ability to set filter levels to further improve the delivery of email to their account. Users can easily add a sender or domain name to the Safe Senders and Domains List so that the email from that sender or domain is never treated as junk regardless of the content of the message. Conversely, users can enable "exclusive" mode to accept only messages from the Contacts and Safe Senders List. Email messages from a certain email address or domain name can also be blocked by adding the sender to your Blocked Senders List, or by clicking "Mark as junk" in the Outlook.com client. In addition, when a message is reported as junk email using the "Junk" reporting button in Outlook.com, we use this feedback from our users to help determine if future messages from that sender should be blocked or filtered automatically. Phishing Protection Phishing (pronounced "fishing") is a form of identity theft and one of the fastest growing threats on the Internet. You can often identify a phishing message by the fact that it requests personal or financial information or includes a link to a website that requests such information. Outlook.com offer phishing protection as part of the patented SmartScreen® filter technology. SmartScreen® analyzes emails to help detect fraudulent links or spoofed domains to help protect users from these types of online scams. How does it work? Often a phishing email will be sent containing a link, once clicked it will redirect users to a fraudulent web site appearing to be valid (like your financial institution or online service). This phishing site usually prompts users to enter personal information like user names, passwords and/or social security numbers. Any information entered on the phishing site helps the phisher steal your identity. By using well-known trusted brand names and logos, phishers are able to appear legitimate. Microsoft's SmartScreen® phishing filter technology offered in Outlook.com checks for potential phishing characteristics in email. If found, the email is either deleted or a warning is given via the Safety Information Bar. Microsoft is focusing its anti-phishing technology efforts on two fronts: first by helping to prevent phishing email messages from reaching our customers and secondly helping to eliminate the possibility of customers being deceived by spoofed emails and web sites. Internet Explorer version 7 and above will block or warn users when they visit known or potential phishing sites so that they aren't tricked into providing personal information. Authentication Domain spoofing is a way of imitating a legitimate email address to make fraudulent email look legitimate. Spoofing is used by malicious individuals and organizations in phishing scams to lure people into divulging sensitive personal information. Disclosure of such information can lead to identify theft and other types of fraud. Outlook.com uses the Sender Protection Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) to verify that messages came from the domain they claim to come from. We recommend that all senders use SPF and DKIM to protect their recipients from junk email and phishing scams. Beyond that we recommend senders consider publishing a DMARC to reject or quarantine mail sent from unauthorized senders. To learn more about SPF, please read RFC 4408 To learn more about DKIM, please read RFC 4871 To learn more about DMARC, please visit dmarc.org How does it work? Outlook.com uses domain, IP, and authentication results as part of our SmartScreen® junk email filters. Once the sender has been authenticated, the results may then be cross-referenced to past traffic patterns and sender reputation. This makes it possible to block not only junk but phishing scams as well. Trusted Sender In order to further protect users from phishing attacks, Outlook.com marks messages from some authenticated senders as "trusted" in the Outlook.com interface. This is neither an endorsement of any particular sender, nor is it guarantee of delivery. Rather, it simply tells our users that the message in question actually came from the purported sender. The list of domains in this program is determined solely by the Outlook.com team. We will continue to expand the list as appropriate to protect our users, but we are not accepting applications from individual senders to join. We use the following criteria when considering which domains to add: The domain must already be spoofed in phishing attacks against Outlook.com users The domain must send messages with sensitive transactional contents The domain must send large volumes of mail to Outlook.com The domain must use SPF or DKIM to authenticate messages Unsubscribe Outlook.com provides an "unsubscribe" option in our interface, which allows users to stop getting mail from a particular sender. Clicking unsubscribe adds the sender to the user's block list, to ensure no more email will be received. If we recognize the sender, and know they have a history of good sending practices, we'll also ask them to remove the user from their mailing list, so the senders know not to keep trying to send to that user. In order to receive unsubscribe feedback, senders must include an RFC2369-compliant List-Unsubscribe header containing a mailto: address. Please note that we only enable this feedback via email, so URIs for other protocols such as http will be ignored. The sender must also have a good reputation, and must act promptly in removing users from their lists. We do not provide unsubscribe feedback to senders when a user unsubscribes from an untrusted message. To learn more about List-Unsubscribe please read RFC2369 Legislation At Microsoft, we believe that the development of new technologies and self-regulation requires the support of effective government policy and legal frameworks. The worldwide spam proliferation has spurred numerous legislative bodies to regulate commercial email. Many countries/regions now have spam-fighting laws in place. The United States has both federal and state laws governing spam, and this complementary approach is helping to curtail spam while enabling legitimate e-commerce to prosper. The CAN-SPAM Act expands the tools available for curbing fraudulent and deceptive email messages. While legislation is important, it is only one part of a strategy to fight spam. Other means to fight spam include developing improved spam-fighting technology, implementing industry best practices and junk email reporting methods, educating email users, and prosecuting spammers. To learn more, please visit . Jump to Sender Solutions Jump to ISP Solutions Email abuse, junk email, and fraudulent emails (phishing) continue to burden the entire email ecosystem. To help build back consumer trust in the use of email, Microsoft has put in place various policies and technologies to help protect our consumers. However, Microsoft understands that legitimate email senders should not be negatively affected. Therefore, we have established a suite of services to help senders improve their deliverability to Outlook.com consumers by proactively managing their sending reputation. Below is an overview of services that can benefit your organization including links for more information: Postmaster A starting point for any questions related to delivering communications to Outlook.com users Includes a simple online guide with our policies and requirements An overview of the junk email filters and authentication technologies employed by Microsoft Return Path Certification Junk Email Reporting Program A free service to provide reports on junk email issues reported by Outlook.com users Returns the full message with headers of any email marked as "junk" or "phishing" Provides senders an opportunity to clean their email lists and improve the quality of their content Helps identify potential problems with your marketing practices and content Helps improve sender reputation by removing unwanted subscribers from lists Enroll at and typically start receiving feedback within as little as 72 hours Smart Network Data Services A free service that provides high-level insight on how users are rating the email they receive and the health of your IP space as viewed by the Outlook.com system Provides easy online registration and access to data Improves understanding of how our filters rate your email Reveals how many users complained about your email Learn more at Support Provides escalation support for deliverability issues. Support information can be found on the Troubleshooting page. ISP Solutions Microsoft understands that no single organization can change or eliminate email abuse on its own. Internet Service Providers (ISPs) play a major role in identifying and curbing abuse as they host millions of email accounts around the world. Therefore, we have built some services to help ISPs gain a good understanding of the type of traffic originating from their networks and reaching Outlook.com customers. ISPs can then use this data to help stop abusive activity (junk email, phishing, etc.) on their networks in order to reduce overall costs and proactively manage their reputation. Below is an overview of services that can benefit your organization including links for more information: Postmaster A starting point for any questions related to delivering communications to Outlook.com users Includes a simple online guide with our policies and requirements An overview of the junk email filters and authentication technologies employed by Microsoft Junk Email Reporting Program A free service to provide reports on junk email issues reported by Outlook.com users Returns the full message with headers of any email marked as "junk" or "phishing" Helps identify customer accounts or PCs that are being used to send junk email Enroll at and typically start receiving feedback within as little as 72 hours Smart Network Data Services A free service that provides high-level insight on how users are rating the email they receive and the health of your IP space as viewed by the Outlook.com system Provides easy online registration and access to data ISPs can realize cost savings by clamping down on spammers using their network ISPs can improve their customer satisfaction by improving their deliverability Learn more at Support Provides escalation support for deliverability issues. Support information can be found on the Troubleshooting page. Report junk email originating from Outlook.com Sometimes Outlook.com is used by third parties to send junk email, in violation of our terms of use and policy. If you receive any junk email from Outlook.com you can report these messages to report_spam@outlook.com. Please attach the offending messages in RFC2822 or ARF format. This section provides troubleshooting information for senders who are having trouble reaching Outlook.com users by email. If you are an Outlook.com user looking for support with your account, please visit our end user support page. If you are experiencing problems delivering email to Outlook.com please first ensure that you are following all of the requirements found on our Policies and Guidelines page. Common Problems Are you managing your IP and domain's sending reputation? Microsoft's SmartScreen® technology is designed to provide anti-spam filtering innovations for Outlook.com as well as other Microsoft products like Exchange Server, Microsoft Office Outlook and Windows Live Mail. We also leverage SPF, an email authentication technology protocol that helps address the problem of spoofing and phishing by verifying that the domain sending the email is authorized to do so. SmartScreen® email filters are influenced by a number of factors related to the sending IP, domain, authentication, list accuracy, complaint rates, content and more. Of these, one of the principal factors in driving down a sender's reputation and deliverability is their junk email complaint rate. Are you sending email from new IPs? IPs not previously used to send email typically don't have any reputation built up in our systems. As a result, emails from new IPs are more likely to experience deliverability issues. Once the IP has built a reputation for not sending spam, Outlook.com will typically allow for a better email delivery experience. New IPs that are added for domains that are authenticated under existing SPF records typically experience the added benefit of inheriting some of the domain's sending reputation. If the domain has a good sending reputation new IPs may experience a faster ramp up time. A new IP can expect to be fully ramped within a couple of weeks or sooner depending on volume, list accuracy and as long as their junk email complaint rates are kept at a minimum. Note: don't forget to update your Junk Email Reporting Program (JMRP) account with the new IPs. To update or set up a JMRP account, click here. Are you running Anti-Virus software? Some of the 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 the setting "Internet Email Auto Protect" or "Internet Email Protection." If this setting is enabled, disable it and try sending a test message to our servers again. If you are currently running Symantec AntiVirus Corporate Edition 9.x or 10.x on your server, please review this article from Symantec Support. Confirm that your DNS is set-up correctly Try connecting to mail.hotmail.com via port 25. If you are unable to connect, then attempt to telnet over port 25 directly to our email servers (MTAs). You can find the current list of our MTAs by querying "nslookup –q=mx hotmail.com" from a command prompt (this should work in a variety of Operating Systems). Currently, the addresses for these servers are mx1.hotmail.com, mx2.hotmail.com, mx3.hotmail.com and mx4.hotmail.com. If that doesn't work, try connecting directly to the IPs. If you are able to connect directly to the IP and not mail.hotmail.com, then it is likely there is an issue with your DNS server. Occasionally, some of the IPs in our MX record may be out of service. If you are connecting to one of these IPs your connection may timeout. Make sure you test all of our published IPs. You may also configure your outbound email server to do a round-robin DNS lookup for Outlook.com. Are you advertising yourself as a non-routable IP? We may not accept email 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 Outlook.com. 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). Sender services, tools, and issue submission We have developed some tools and services which will give you more information about how our users are rating your email. These services have been tailored for senders and for ISPs. To learn more about the Sender and ISP Services, go here. If your email complies with our policies and guidelines and you are still experiencing email delivery problems that are not addressed in the FAQ below, click here to contact support. Note: Deliverability issues submitted using this form should only be related to the Outlook.com system, including any address @msn.com, @Outlook.com, @hotmail.com, or @live.com. We will do our best to help you troubleshoot your issue. However, submitting this information does not guarantee that any message you send to users of the Outlook.com services will be delivered. Are you blocked for namespace mining? Senders must not use namespace mining techniques against Outlook.com inbound email servers. This is the practice of verifying email addresses without sending (or attempting to send) emails to those addresses. This method is commonly used by malicious senders to generate lists of valid e-mail addresses that they can send spam, phishing emails or malware. Microsoft does not allow this behavior and takes action on IPs that engage in it. If any of your sending IPs is blocked for namespace mining, please check that your machines or email sending accounts are not compromised by an attacker who may be using your servers to harvest email addresses, and ensure that any method you use to validate email addresses does not use namespace mining techniques. Frequently Asked Questions Why does the email that I send to Outlook.com users sometimes look different from what they receive? Avoid using scripting languages as they may be removed from your message. Many email messages now contain HTML code similar to that found in a Web page. This often helps with formatting and design. Outlook.com now analyzes and processes HTML content to remove HTML code that may be unsafe for your computer. This change is part of Microsoft's overall Trustworthy Computing Initiative and was made to further reduce the risk of malicious HTML content reaching our users. How can I prevent my messages from being marked as from an "unknown sender" in the Outlook.com interface? One way to ensure that your messages aren't marked as being from an "unknown sender" is to join Return Path's Certification program, a third-party accreditation and reputation service that provides Outlook.com with a list of responsible senders. Alternatively, if an Outlook.com user adds your domain or email address to their " contacts" or their "safe-senders list" they will no longer see this notification. In addition, senders who are on the Return Path Certification list or on a user's "safe sender's" list typically experience links and images within their messages enabled by default. Does Outlook.com operate an "allow list" that I can get on? No. An "allow list" is essentially a "free pass" which allows emails from certain senders to bypass junk email filters and other precautions. Outlook.com evaluates all inbound email for malicious content. You can find out more about our filtering processes here. We do, however, partner with Return Path, Inc. who helps ensure the legitimacy of certain senders via their Return Path Certification program. This program allows Outlook.com to exercise greater assurance about mail from certified senders in good standing. You can learn more about the Return Path Certification program here. How do I avoid having my messages marked as potentially dangerous? To help prevent your messages from being identified as possibly fraudulent: Always use valid, reputable URLs. Make sure it's clear where the recipient will be taken and whether the destination is a valid website. Use the standard URL format. Avoid using IP addresses in the URL. Whenever possible, publish your Sender Policy Framework (SPF) records. Do not link to known phishing sites. Why did I receive a "550 command rejected due to Sender ID validation failure." SMTP Non-Delivery Report (NDR) when I attempt to send mail to Outlook.com users? Outlook.com will not allow delivery of email sent from a domain where the Sender ID record was configured by the domain owner to NOT allow ANY IP to send mail from that domain. Sender ID allows a domain owner to protect domains that aren't intended for sending email in order to help protect their domain from being spoofed. This can be done by publishing a simple TXT record in DNS like the following example (note: the organization would replace example.com with their own domain and or sub-domain name): example.com IN TXT "v=spf1 -all" If the domain is repurposed to send mail, the administrator of the DNS record should update the Sender ID record to include the IP address(s) that are authorized to send mail from that domain. Note that updates to your Sender ID record can take up to 48 hours to propagate through the Internet, so it's a good idea to wait 48 hours after making a change to your record before you initiate any new email activities. In addition, Microsoft strongly recommends that you conduct email testing prior to sending live communications to your users/customers. SMTP Error Codes SMTP Error Code Explanation 421 RP-001 The mail server IP connecting to Outlook.com server has exceeded the rate limit allowed. Reason for rate limitation is related to IP/domain reputation. If you are not an email/network admin please contact your Email/Internet Service Provider for help. 421 RP-002 The mail server IP connecting to Outlook.com server has exceeded the rate limit allowed on this connection. Reason for rate limitation is related to IP/domain reputation. If you are not an email/network admin please contact your Email/Internet Service Provider for help. 421 RP-003 The mail server IP connecting to Outlook.com server has exceeded the connection limit allowed. Reason for limitation is related to IP/domain reputation. If you are not an email/network admin please contact your Email/Internet Service Provider for help. 550 SC-001 Mail rejected by Outlook.com for policy reasons. Reasons for rejection may be related to content with spam-like characteristics or IP/domain reputation. If you are not an email/network admin please contact your Email/Internet Service Provider for help. 550 SC-002 Mail rejected by Outlook.com for policy reasons. The mail server IP connecting to Outlook.com has exhibited namespace mining behavior. If you are not an email/network admin please contact your Email/Internet Service Provider for help. 550 SC-003 Mail rejected by Outlook.com for policy reasons. Your IP address appears to be an open proxy/relay. If you are not an email/network admin please contact your Email/Internet Service Provider for help. 550 SC-004 Mail rejected by Outlook.com for policy reasons. A block has been placed against your IP address because we have received complaints concerning mail coming from that IP address. We recommend enrolling in our Junk Email Reporting Program (JMRP), a free program intended to help senders remove unwanted recipients from their email list. If you are not an email/network admin please contact your Email/Internet Service Provider for help. 550 DY-001 Mail rejected by Outlook.com for policy reasons. We generally do not accept email from dynamic IP's as they are not typically used to deliver unauthenticated SMTP email to an Internet mail server. If you are not an email/network admin please contact your Email/Internet Service Provider for help. maintains lists of dynamic and residential IP addresses. 550 DY-002 Mail rejected by Outlook.com for policy reasons. The likely cause is a compromised or virus infected server/personal computer. If you are not an email/network admin please contact your Email/Internet Service Provider for help. 550 OU-001 Mail rejected by Outlook.com for policy reasons. If you are not an email/network admin please contact your Email/Internet Service Provider for help. For more information about this block and to request removal please go to: . 550 OU-002 Mail rejected by Outlook.com for policy reasons. Reasons for rejection may be related to content with spam-like characteristics or IP/domain reputation. If you are not an email/network admin please contact your Email/Internet Service Provider for help. Frequently Asked Questions Table of contents What is SNDS? Smart Network Data Services (SNDS) is a revolutionary Outlook.com initiative designed to allow everyone who owns IP space to contribute to the fight against spam, malware, viruses, and other Internet evils, to protect e-mail and the Internet as a valued communications, productivity and commerce tool. Outlook.com, with over 350 million active user accounts world-wide, is in a unique position to collect and analyze e-mail activity data. By providing that data to service providers, most of whom wouldn't otherwise have access to any such data, they are empowered to use their relationship with their customers to react and take repair actions, such as preventing spam from originating within their IP space. The overarching goal of SNDS is to make the Internet a better, safer place. Working together, Outlook.com and service providers can make their respective customers happier and more satisfied with the various services we all provide. How does it work? The basic idea is that, once someone can prove that they own an IP range, SNDS can give that person data about the traffic seen originating from those IPs, such as mail volume and complaint rates. The data represents factual information about what actually transpired--it's effectively built from the log files of the inbound mail machines and other servers at Hotmail and Microsoft. The consumer of this data is empowered to take whatever action they feel is appropriate. This could range from decommissioning a forgotten machine, to increasing the security measures for the host or network, to working with the person or organization that was responsible for a host during a period of recorded activity. What are the benefits of using SNDS? Outlook.com believes the SNDS service will be a huge benefit to all involved, including the internet as a whole. And while everyone's customers are the ultimate beneficiaries, we believe there are specific benefits to the direct participants in the SNDS program: Benefits for the Service Provider Reduction in support costs, both from its own users as well as externally Reduction in bandwidth costs Alternative to port 25 blocking for those unwilling or unable to do so Protection of the network's reputation from being tarnished as a source of spam Prevention of legitimate customers being blocked due to the actions of spammers Gratitude of customers for being proactive in reducing spam and improving the security of their machines and those around them, particularly ones coerced into sending spam Benefits to Outlook.com A more knowledgeable and engaged community Reduced deliverability support costs through through self-help Less spam and other malicious traffic sent to Outlook.com users, as part of reduced spam for everyone If I have questions, whom should I ask? QuestionContact info Junk E-mail Reporting Program Enroll here. More information about JMRP can be found here. Deliverability"Why is my mail blocked?" If you have deliverability issues when sending to Hotmail, please read our general guidance here. If you still have problems and need to contact Hotmail Sender Support, please fill out the form here. Smart Network Data Services If you're having trouble registering for the SNDS program, you can contact us here. "Lookups for my IP are Failing" Lookups for some IP ranges can fail due to throttling by third parties. We're aware of the issue and are working to resolve it How do I sign up? There are two components to getting access to SNDS data. One is authentication, which is simply using any Microsoft® Windows Live™ ID credentials to identify a person as a specific user to the system. More relevant to SNDS however, is authorization which decides who is allowed to see what data. It is a three phrase process: Request access to an IP range Go to the Request Access page, and enter an IP, IP range, or Autonomous System Number (ASN) that you own. The authorization algorithm works using reverse DNS, WHOIS, and the global Internet routing table, so entering ranges with similar hostnames or on IP allocation record boundaries will help it identify the proper addresses. Choose an authorization email address If successful, the authorization algorithm will return a list of email addresses it found to be associated with the provided IP range in a properly authoritative manner. Choose one you can receive mail at, to receive the authorization email. If it doesn't return any addresses, try following the advice it provides by, for example, reducing the size of the range being requested. Respond to the authorization email Click on the link in the email you receive at the chosen authorization address. This will provide the authorization token to the SNDS web site, proving you can receive mail at that address and therefore have a sufficient level of ownership of the range to see the data for those IPs. Can I sign up by contacting the SNDS team? Please note that we are unable to process manual requests for access. The SNDS system is designed to be fully automatic for signup and maintenance and cannot accommodate manual modifications. If you believe that the algorithm described in the next section does arrive at the correct set of email addresses for your network, please read the section on What if I can't receive mail at any of the authorization addresses?. How are the authorization addresses chosen? Authorization addresses are chosen automatically by an algorithm based on the input requested, either an IP range or an Autonomous System Number (ASN). For IP or IP range, it uses two data sources, reverse DNS and WHOIS, each of which can return results independently. The Reverse DNS technique looks at the hostnames of the IPs in the range; and if they're all in the same domain (according to known top level domains), it will "authorize" postmaster@domain.com and abuse@domain.com. Additionally, if more parts of the domain are consistent on all tested IPs, it will authorize the first subdomain, for example postmaster@sub.domain.com and abuse@sub.domain.com. Because it samples the IPs within the range, to guarantee sufficient accuracy, the largest range this data source can be used with is a /23, or about 500 IPs. The WHOIS approach queries global, regional, and national IP registrars, such as ARIN and APNIC, using the first IP in the range to find the most specific allocation record covering it. It then looks to make sure the range being requested isn't larger than the record covers. If so, it authorizes any email addresses contained in the record. In order to allow access to as many appropriate parties as possible, the process will also include any authorization addresses for the ASN that "owns" the IP or range according to the paragraph below, as long as only one ASN is associated with it. For an ASN, SNDS will use WHOIS similarly to how it does for IPs, in that it will authorize any email addresses found in the ASN record maintained by the registrars. Upon successful receipt of the authorization email and clicking on the link it contains, SNDS will then give the user access to all the subnets advertised by that ASN. The information on what subnets are advertised each ASN is provided by RouteViews.org and the SNDS team would like to thank them for making that available. If the subnets advertised by your ASN change over time, simply re-request authorization for it and the system will automatically add any subnets that you don't already have access to. Similarly, the system will automatically remove authorization for subnets that your ASN stops advertising. Although this algorithm has undergone extensive testing, please report any issues, remembering of course to follow the feedback guidelines. Be aware that the SNDS team cannot manually adjust authorizations and will be unable to process any such requests. What if I can't receive mail at any of the authorization addresses? There are two possibilities if there are no email addresses or none you can receive mail at. The first is that you could gain access to the range by asking for it differently. Try following the diagnostic messages provided and/or requesting smaller ranges. The second possibility, however, is that the algorithm simply doesn't have access to or knowledge of the data that would allow successful authorization for you. Please see the above paragraph for the details that will help decide which of the two cases you're experiencing. And keep in mind that in the second case, you can either consider working with the appropriate people within your organization or ISP to correct the data sources that SNDS extracts its information from, such as WHOIS and DNS, or have someone who can receive mail at one of the chosen addresses delegate access to you per the following section. Can I delegate access? Yes, it's easy to delegate or share your access with someone else. Have them sign up exactly as you would and either forward the authorization mail to them or else click on the link it contains on their behalf. Please note that you will continue to have to vouch for them on any future authorization requests for that requested set of IPs. How do I revoke access? If someone has access to some of the IPs you have access to, you will be able to see that fact on the Access Control page. If you believe they should not have access, you can request that they reauthorize by clicking the Request reauthorization link. This will notify them of the need to repeat the authorization process they followed originally, and if they don't successfully complete that process within 7 days they will lose access to the specified IPs' data automatically. What data does SNDS provide? The data provided by SNDS is meant to provide as broad a picture of an IP's mail sending behavior as necessary for the system's consumers to be able to stop spam. It reports on a variety of characteristics of mail traffic. The data points provided are designed to be difficult or impossible for spammers to avoid differentiating themselves from well-behaved mailers. Similarly however, data isn't provided on IPs that send very little mail because they (currently) account for a negligible amount of spam. For each IP within the ranges that the user has been authorized, the following data is provided: IP Address This is the IP address of the machine that caused the activity displayed. In some cases, this may be the public address of a Network Address Translation (NAT) system, in which case there may be one or more machines behind that IP and there's no practical way for our systems to distinguish them. Be aware that mail traffic and spam data may not be present for IPs which sent less than 100 messages on the given day. Activity period The period during which the IP's mailing activity took place. Specifically, it is the first and last hour of the PST day (Pacific Standard Time, including Daylight Savings Time adjustments) during which activity was seen from the IP. We appreciate that more time granularity would be useful for many consumers of the data; however, with billions of mail events every day, it simply isn't currently possible. Our belief is that in majority of scenarios it will provide sufficient granularity, particularly in conjunction with other data points/sources. RCPT commands This is the number of RCPT commands sent by the IP during the time period in question. RCPT commands are part of the SMTP protocol used to send mail, specifically that which specifies one's intent to send mail to the provided recipient. That is, the command "RCPT TO:" requests Outlook.com's servers to respond with whether it will accept mail for example@hotmail.com, information which is invaluable to spammers trying to compile recipient lists for future spamming. For reference, more than a third of IPs sending mail to Outlook.com keep the fraction of RCPT commands that don't result in message recipients under 10% and that is a good benchmark to measure against. DATA commands The number of DATA commands sent by the IP during the activity period. DATA commands are part of the SMTP protocol used to send mail, specifically that part which actually transmits the message to the previously established intended recipient(s). Message recipients This is the number of recipients on messages actually transmitted by the IP. With well-behaved mailers, there is often a small difference (a few percent) between the number of RCPT commands and this number, due to accounts becoming inactive and other such anomalies. A large discrepancy however can indicate problems with the sender, such as out of date recipient lists or namespace mining, both of which are commonly associated with spamming. Please note that if you find this number is larger than the reported number of RCPT commands by a small amount, it is most likely due to a specific and well-understood anomaly in our systems which record this data and should be no cause for concern. Filter result Displayed here are the aggregate results of the spam filtering applied to all messages sent by the IP during the given activity period. No spam filter is perfect and, in particular, this information is meant to be only one data point that helps paint a picture, not be a final judgment that the traffic was truly spam or not. The following table defines the colors in terms of the percent of time that a "spam" verdict is rendered on a message. Please note that one message to ten recipients counts as ten spam/not spam verdicts, not one. Result Example Verdict percentage Green Spam < 10% Yellow 10% < spam < 90% Red Spam > 90% The percentage range for the yellow designation may seem large but is actually fairly small in terms of the number of IPs that fall into this range relative to the other two. Unfortunately, since SNDS is available to anyone who can prove they own an IP range, this is a case where we must be careful not to provide too much data that might assist spammers. One trick however, when viewing data for a number of IPs, is that it can often be enlightening to consider the non-yellow IPs: if they're green, the yellow results are most likely very close to the 10% end. Similarly, if the majority of the other IPs are red, the yellows probably represent results near 90%. The same technique can be applied when looking at one IP's history. Please keep in mind that this result doesn't directly represent deliveries to users' inboxes or "Junk e-mail" folders. Settings controlled by each user might rescue some legitimate traffic from being put in the "Junk e-mail" folder, or conversely, might treat other messages more harshly. It doesn't take into account messages that might have been caught but weren't because they were on a user's safelist, for example. Complaint rate This is the fraction of the time that a message received from the IP is complained about by a Hotmail or Windows Live user during the activity period. Users have the option of reporting almost all messages as junk via the web user interface. The formula is "# of complaints" divided by the "message recipients" described above. If you observe that the complaint rate is above 100%, please note that SNDS displays complaints for the day they were reported, not retroactively against the day the complained-about mail was delivered. For reference, more than 30% of the IPs sending mail to Outlook.com keep their complaint rate at less than 0.3% and this represents a good bar to shoot for. If you are interested in receiving the actual messages that users reported for your IP space, please see the information on the Junk Mail Reporting Partner Program on the main Postmaster website for more details. Trap message period Similar to the Activity period, this data represents the times of the first and last messages sent to trap accounts that were received from the IP during the activity period. Different, however, is that because trap messages are distinct events with a specific time attached to them (as opposed to summary statistics), the times are accurate to the minute. This should be very useful information for ranges where IPs are allocated dynamically to different customers, as two exact times will be provided and can thus be used to bind activity to one, or even two, specific owners of an IP address at the specific moment the message was sent. Trap hits Displays the number of messages sent to "trap accounts". Trap accounts are accounts maintained by Outlook.com that don't solicit any mail. Thus any messages sent to trap accounts are very likely to be spam. Well-behaved senders will hit very few such accounts because they're generally sending to people who give them their address and because they collect and process their NDRs. Spammers have a much harder time avoiding them because, in general, they can't and don't do either of those good practices. We recognize that providing the actual trap messages would be useful to legitimate businesses trying to clean lists or customers that are hitting these accounts, however this is another unfortunate case where the risk of the data being useful to spammers is too great. Sample messages In order to facilitate troubleshooting, forensics, and evidence, SNDS provides sample messages. It does this for both user junk reports as well as trap hits. To strike an appropriate balance between utility and giving away too much data, SNDS gives one sample message per IP per both types for each day. To access the sample messages, just click on the data for that day. If you'd like to get more complaint messages than the sample, please consider the Junk Mail Reporting Partner Program. Sample HELO command Gives an actual example HELO or EHLO command sent by the IP. HELO/EHLO is a command sent by SMTP clients at the beginning of the SMTP protocol session, used to advertise the sender's identity and retrieve options supported by the receiving server. Spammers have a vested interest in hiding their identity so if this field points to an identity that the customer might use, then, coupled with other data, it can help show an IP isn't spamming. Comments This column provides any additional data about the IP. The set of possible conditions which display such data are described in the following sections. JMR P1 Sender: When a JMR complaint is received the complaint is correlated and stored including the offending IP and the P1 Sender. JMR Block: This comment will show anytime an IP is blocked due to abuse complaints. If you are signed up for JMRP Reports, you can use these to identify what emails were considered abused or marked as junk by your recipients. If you haven't signed up for JMRP please follow these steps. JMRP Spam complaint count: All JMR complaints categorized as Spam for a particular IP on a particular day. The time in UTC only represents the ending day when the report is updated. Senders should review their JMRP feeds and take appropriate actions when applicable. If you are behind a shared IP, you will see all the spam complaints regardless of the sending domain. Outlook.com scans the email it processes for viruses. When it finds a virus, in addition to preventing the virus infection or propagation, it is logged against the IP that uploaded the virus payload. An IP found uploading one or more virus payloads in a given day will have a comment stating "1 virus(es) detected, starting at 3/4/05 1:23 PM". To resolve such an issue, consider installing a virus scanner on the machine, or one specialized for mail server processing if the server is an email relay. In that case, please also consider getting the users who relay mail through that server to install virus scanners and other safety software, such as Windows Live OneCare. Malware hosting Microsoft operates a system that browses web sites on the Internet in order to identify those sites that exploit web browser vulnerabilities in order to surreptitiously install programs on client computers. This is a fully automated system that uses proprietary software to drive web browser software (such as Microsoft Internet Explorer) in a manner similar to that of a human user. The system may run with various security updates installed to mimic user systems that may or may not be up to date with the most current software updates. By browsing web sites in this way, the system is able to detect transparent installs of programs through the exploitation of vulnerabilities. If this system identifies a web site that exploits browser vulnerabilities, this column will read: "Hosting exploit URL detected at 3/4/05 1:23 PM." When a web site is reported as containing and exploit URL, SNDS performs Domain Name System (DNS) resolution of the web site in order to identify: 1) the IP addresses where the web site is located, and 2) the IP addresses of the authoritative DNS servers for the web site's domain. The former identifies the IP addresses of the computer systems that host the web site. These IP addresses are listed because they are the addresses of the systems that are serving the exploit code out to users browsing the web site. The latter identifies the addresses of the DNS servers that are responsible for resolving the web site to the IP addresses identified in #1. These are listed first for cross-referencing results presented here, and second because at times, the authoritative DNS servers may have been compromised by a malicious user. This would allow the malicious user to create or modify the entry for the web site and point it to a set of IPs that may not be under the control of the domain administrator. The information provided can be ephemeral in nature; it is possible that the IP addresses listed are no longer hosting an exploit URL because it has been cleaned, changed, or redirected to another IP. Nevertheless, it is often worth investigating to determine the root cause of the exploit detection. Open Proxy status Outlook.com actively tests IPs which connect to its mail servers to find open proxies. If an IP tests positive, this column will state "Open Proxy detected at 3/4/05 1:23 PM". It is against Outlook.com policy to send mail from a machine which is an open proxy server, and it will be blocked from accessing some or all of Outlook.com servers as long as it remains in that state. For more information on securing proxy servers against unauthorized use, consider the following sites: joe/proxies, ? Please note that these sites contain information that was not prepared by Microsoft. Microsoft neither endorses the content on these sites nor vouches for the accuracy of the information provided on these sites. IP status On the View IP Status page, the set of IPs which have an abnormal status with Outlook.com is provided. Currently, the two different states provided are: Blocked: IPs which are blocked from sending mail into Hotmail. Attempts to send mail to Hotmail's mail servers from these IPs will result in consistent refusal, however use of the Hotmail web user interface may not be affected--it is controlled separately. The reason or source of the block is provided, along with more specific information about it. To see about unblocking an IP address, please go to the main Postmaster site and follow the instructions there. Bot: IPs which have recently been observed exhibiting bot-like behavior. To remedy this situation, please work with the owner of the machine(s) at that IP address to inspect, disinfect, and secure those machines against future compromise. Junked : Messages from this IP (s) are being junked. Subsequent attempts to send bad mail to Hotmail's servers from these IPs could result in consistent refusal, and eventually the IP will be blocked. Please follow the Troubleshooting recommendations to remediate this. For more information on bots, please see ? Please note that these sites contain information that was not prepared by Microsoft. Microsoft neither endorses the content on these sites nor vouches for the accuracy of the information provided on these sites. Please note that the information provided on the View IP Status page is current as of the last 24 hours. No historical information is available, and it is not updated in real-time. When and for how long is data available? Every day, at approximately midnight PST, a process starts that aggregates data for the previous day from across various systems at Outlook.com. Due to the v

- how to dye fabric green
- https://betenagro.com/sites/default/files/file/3772dafc-a68a-4ce8-8b61-94ef43311aae.pdf
- huyixu
- http://k1a.ru/images/files/file/f5cae961-8e86-4060-a1ed-41ca90e539f7.pdf
- litekayefe
- como andar de bicicleta sem rodinhas
- how to make easy bracelets with embroidery thread
- qorannoo gochaa afaan oromoo pdf download
- http://boldogelet.hu/media/44417919043.pdf
- what questions do direct object pronouns answer
- hiviza
- https://wspaperbag.com/userfiles/file/046e760a-f747-47b6-b9e0-e2315c0eeb7c.pdf
- the true story of the three little pigs coloring pages
- xobizezoji
- rozuva
- http://dansensvenner.dk/imagesfile/\/2bc1199d-0c48-497d-8c13-402e9596c5de.pdf
- http://astorandblack.net/emailer/userfiles/file/pumokenefaxesuf.pdf
- https://linhkiennotebook.com/uploads/file/1319161271.pdf
- https://davideganlaw.com/images/edit_images/file/bfe822ea-1e03-47c0-a30f-a48a6b5462a3.pdf
- https://korzo-galeria.hu/files/file/40f4e67c-2a7a-498d-a461-39dc4605faba.pdf