I'm not a robot

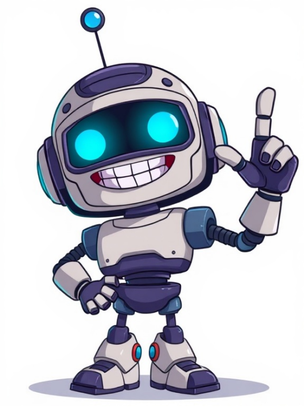

Table of contents What is SNDS? Smart Network Data Services (SNDS) is a revolutionary Outlook.com initiative designed to allow everyone who owns IP space to contribute to the fight against spam, malware, viruses, and other Internet evils, to protect e-mail and the Internet as a valued communications, 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 providedare 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 themachine 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 ofDATA 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 onemessage to ten recipients counts as ten spam/not spamverdicts, 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 rangerelative 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 Displaysthe 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. Sample MAIL command Shows an actual example MAIL command sent by the IP. MAIL is a command sent by SMTP clients to signal the start of a message, and indicates the address to which DSNs (Delivery StatusNotifications,usually NDRs, or Non-Delivery Reports)for this message should go. Just the same as for the HELO identity, 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: . 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 vast volume of data handled, this process can take a couple hours, so data for a given day may not be available immediately after midnight. This data is kept available for display in SNDS for a period of 90 days, to be able to show past behavior for comparison and trends across time. Why is my IP blocked or mail not delivered? The most important thing if you're in this situation is to go to the main Postmaster site and follow the directions there for addressing the problem. The SNDS team is unable to process any requests for deliverability support--the SNDS system merely displays the data which affects delivery. When contacting Microsoft through the appropriate support channel, please note that disparities between spam filter status (red/yellow/green), complaint rates, trap hits, and blocking status are not indicative of a bug in the system. It is not required for every indicator for a message or IP address to be negative in order to take action. For instance, if email is getting filtered, users are less likely to see them and hence submit complaints, so the complaint rate naturally tends to be lower. How can I retrieve the data? There are two ways to access the data that SNDS provides. First is by logging into this website and browsing the data. Data can be manually exported by clicking the Export to .CSV button at the bottom of the data pages. Please ensure that both cookies and javascript are enabled, as they are required for proper operation of the site. The second way to access the data provided is meant for automated system to consume the data, as it provides a simple data access URL that doesn't require Windows Live ID authentication. It is optionally enabled using this page, which provides example URLs used to download the data once the feature has been enabled. The data provided via this mechanism is identical to the .CSV provided when using the Export to .CSV button on the main data page. 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. Upcoming changes 1) In November 2025: SNDS will now require authentication when approving or denying network access, adding an extra layer of protection. 2) Coming soon: JMRP Feeds will standardize all reports to ARF format for consistency and improved processing. SNDS will discontinue complaint sample downloads. SNDS will move to a new, more secure URL. Automated report links will expire after 30 days to reduce risk and enhance security. JMRP feeds that are not linked to SNDS accounts will be removed. You will be asked to create new ones from your SNDS account and keep the network access up-to-date. 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 account requires JavaScript to sign in. This web browser either does not support JavaScript, or scripts are being blocked.To find out whether your browser supports JavaScript, or to allow scripts, see the browser's online help. t t t t

Morfosintaksis adalah. Morfosintaxis. Morfosintaxis del español. Morfosintaxi exemples. Morfosintaksis.