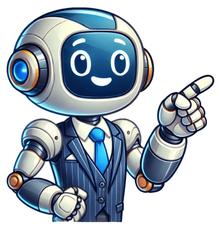
Continue



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. Microsoft is dedicated to help provide the most trusted and protected consumer experience on the web. Therefore, Microsoft has developed various policies, procedures, and adopted several industry best practices to help protect our consumers from abusive, unwanted or malicious email. Senders attempting to send email to Outlook.com users should ensure they fully understand and are following the guidance on this page to help in this effort and to help avoid potential deliverability issues. Email sent to Outlook.com users must comply with all Microsoft policies governing email transmission and use of Outlook.com. Microsoft Services Agreement Microsoft Anti-Spam Policy Email sent to Outlook.com users must adhere to all applicable laws and regulations governing email communications in the applicable jurisdiction. CAN-SPAM Act Email Marketers Must Honor "Unsubscribe" Claims Email sent to Outlook.com should comply with the applicable recommendations listed in the documents below (some links are only available in English) In addition, email servers connecting to Outlook.com must adhere to the following requirements: Sender is expected to comply with all technical standards for the transmission of Internet email, as published by The Internet Society's Internet Engineering Task Force (IETF), including RFC 2821, RFC 2822, and others. After given a numeric SMTP error response code between 500 and 599 (also known as a permanent non-delivery response), the sender must not attempt to retransmit that message to that recipient. After multiple non-delivery responses (see #2), the sender must cease further attempts to send email to that recipient. Sender must not open more than 500 simultaneous connections to Outlook.com inbound email servers without making prior arrangements. Messages must not be transmitted through insecure email relay or proxy servers. The mechanism for unsubscribing, either from individual lists or all lists hosted by the sender, must be clearly documented and easy for recipients to find and use. Connections from dynamic IP space may not be accepted.. Email servers must have valid reverse DNS records. 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. Email sent to Outlook.com users should include Sender ID authentication. While, other forms of authentication are available, Microsoft currently only validates inbound mail via SPF and Sender ID authentication. Senders, ISP's and other third party senders and service providers should actively manage the reputation of your outbound IPs. Outlook.com has developed the following free services to help in this effort. Junk Email Reporting Program (JMRP) Smart Network Data Services (SNDS) If you are adhering to the guidelines, practices and policies presented on this page and are still experiencing deliverability issues, please contact Outlook.com deliverability support. If you are not in compliance with the above policies and guidelines, it may not be possible for our support team to assist you. Outlook.com Deliverability Support Microsoft actively works with industry bodies and service providers in order to improve the internet/email ecosystem. These organizations have published best practice documents that we support and recommend senders adhere to. This improves your deliverability amongst several email service providers around the world. To report unlawful, abusive, unwanted or malicious email that you find originating from an Outlook.com, Hotmail, Live, or MSN account, please forward a complete copy of the abusive message (including the full message header) to abuse@outlook.com. Sending these types of communications is a violation of Microsoft policy and appropriate action will be taken on confirmed reports. If you are a member of law enforcement and wish to serve Microsoft Corporation with legal documentation regarding an Outlook.com account, or if you have questions regarding legal documentation you have submitted to Microsoft, please call (1) (425) 722-1299. t t t t 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. t t t t 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 . t t t t

Literary devices used in the sun rising. Literary devices in mama is a sunrise. Literary devices in all summer in a day. Literary devices in the sunne rising. Literary devices in still i rise. Literary devices in like the sun. Literary devices in the sun rising by john donne.